目次

前　言

1990年3月4日，我冲了个澡。

这倒不算什么了不起的事儿，那天甚至不是个礼拜六。但这个澡在我的意识中很突出，它是一个起点，对我，对这个国家，都意味着一个崭新的开端。事实上，对世界各地成千上万人所将从事的一门新兴行业来说，也是一个崭新的开端。

这个澡起初和别的澡没啥两样，湿润、温暖，滚滚水流像小瀑布一般喷洒在我头上。棒极了，因为我正在极尽能事地思考。

在这个特殊的三月清晨，我的思绪漫游不定，我懒洋洋地坠入了半梦半醒之间。在这介于沉睡与清醒分野不确定状态下，人们简直能够发誓说作的梦是真的。在梦里，一辈子活生生的经历只消半分钟就展露无遗。

但这个“梦”，你愿意的话也可以说是“幻想”，与众不同。它和山啊、湖啊、松树啊，那些电影《音乐之声》的背景无关，这是一个关于战争的梦。

我看见一种具有拟人化成份的计算机病毒“聪明”地锁定了它的下一个牺牲品。我看见这种病毒召集一切盟友，在符号逻辑的支持和增援下，对毫不知情的牺牲品逐个发起突然攻击。而随着病毒大军的浩荡行进，这些牺牲品一个个无助地俯伏尘埃。

水流继续如瀑布般喷洒，战争在我意识面前展开：“嗅探”软件随后加入了病毒群。这是为窃听而设计的软件，即便受到最严密保护的机密，它也能带着隐蔽地逃逸。数字化骑兵疾速冲了过来，带着更恶毒的用来控制整个网络的程序，和其它战斗部队一道齐心协力，共同作战。

这还不是结局。在我脑海中放映的这部电影进入第二幕，我看得完全着了魔，很想知道这些意念从何处来，又在往何处去。居心不良的硅芯片和其它虚拟战士一道加入闪电战，战胜了我臆想中的牺牲品。

水凉了下来。在这个还没来得及喝口咖啡的清晨，迷迷糊糊的梦境竟如此逼真，我深受震撼。至今一切犹历历在目，我能一幕一幕地重新搬演。

而且，我把它称作：信息战争。

1989 年，我在《安全杂志》和其它安全领域的刊物上发表文章，解释计算机病毒如何能够不需要感染软件程序本身，就埋伏在文字处理、电子数据表和数据库里。我预言，这将演变成一个可怕的问题，并就此提出一些解决办法。文章遭到质疑。

现在呢？时至今日，宇宏病毒以十倍的增长速度成为规模最大的恶意软件业。

1991年6月，国会邀请我作证时，五角大楼没有警告我说，我正涉足于某些机密领域；五角大楼也没有告诉我，他们实在不情愿让一个私营部门人士掌握他们最深层的秘密。政府要求我到众议员丹·格利克曼主持的正在审查计算机安全法的委员会去，“把众议员们彻底给震一下。”我就带着这样的想法准备了一份声明交上去，期望它表达出我对当前安全状况的看法。

我对委员会说，“如果我们不开始认真对待安全问题，我们就面临着电子珍珠港事件的前景。”我不想让那天在场的发言者难堪，不过他们所有人都说：“施瓦陶先生对形势估计过头了。”他们不相信我提出的预测更清醒明智。今天，无一例外地，这些人都因投资于基于这些预测的产品研发而赚了大钱，因为这些预测全都一步一步地变成了现实。

昨日，是信息安全；今天，是信息战争。

1994年4月，英国试图查禁我就此撰写的第一本著作，但没能成功。该书颇引起一些轰动，后果之一是：我本来应邀在几十个严格保密的美国军事机构里发表演讲，而后突然一下子就得不到邀请了——“因为五角大楼里某某不欢迎你。”过了几个月，有的让我过了几年，我才得以进入这些机构的第二道门。我在军界和情报界的支持者不得不履行非常措施以便让我通过警卫，进入

那些从不公开其存在的建筑。在一栋被列为超级机密、完全用首字母标注的大楼里，他们派给我两名武装警卫，下令："如果此人距离计算机不到 20 英尺，格杀勿论。"真该死，幸亏男厕所用的是手动抽水马桶！

事情就这样过去了。后来，到 1997 年 4 月，微软—全国广播公司（MS—NBC）在网上发布一个头条，题目是："信息战争是神话吗？"装饰性标题说明为："一个精心构筑的骗局？"绝大多数传媒当时尚未加以报道。

但我终于得到个人所能得到的最大褒扬：克林顿总统创建了基础设施保护任务部队，以寻求对抗平民信息战争的机制。这是国家安全政策概念上的一个纪念碑。承认美国事实上面临众多新的威胁并必须对此作出迅速反应，这终于成为美国政治架构的一部分。

在昨天的未来成为今天的头版头条之际，我想到明天。有家军事机构来访并询问我："2010 年的信息战争将是个什么样子？"我回答说："如果你等待那么久，我们就输了。"

今年盛夏，一群军事和情报专家让我飞到一片孤零零的沼泽地里，问我 2020 年和 2025 年的战争将如何进行。我告诉他们，"你们将几乎没有依靠，也几乎没有能力作战。你们将无力反击侵略者，因为他们比以往更加暗藏不露，他们的武器所攻击的将不是桥梁、飞机或者计算机。未来的战争将重新成为一群人对一群人、一个人对一个人的战争，完全绕过传统的民族国家。未来

的战争不是核战争，但是每个人都将拥有可以摧毁甚至熔解其邻居的武器。”此情此景带了几分《圣经·启示录》的味道，我随后描述了能造成这种状况的技术。

有太多的人至今仍然相信，信息战争，或曰网络谍报战，或者随便你安它一个什么名字，是一个荒诞的神话。让·吉内尔——我引以为豪的朋友兼战友——所写的这本了不起的书，证明这种局面已经有所改善。

初读让的著作，我身心松弛，大为倾倒，对他所取得的成就备感惊奇。他抉取了一个高度复杂、涉及到许多不同方面的题目，而叙述得却如此清楚简练，通俗易懂。让对信息战争作了出色的分类，提到一定高度，使得每个人都能看出这些问题对于我们的国家地位乃至生存有多么重要。

第一类：个人信息战。在网络空间，你在被证实无辜之前都是有罪的。

第二类：经济和工业谍报战。美国政府的政策如此宽松，以致于我们根本就在鼓励和邀请别国搞这方面的谍报。

第三类：恐怖主义、军事、民间电子防卫、基础设施的崩溃。

让使这一切都变得简单、亲切、明了。他抓住了第二类信息战争本质中的一些关键方面，所讲的故事连我80多岁的丽比阿姨都乐于倾听并且听得懂。

我得脱帽向让·吉内尔致敬。就我迄今所见，《互联

网上的间谍战》一书最清晰地浓缩了信息战争、网络恐怖主义和计算机谍报战的历史，可读性最强。对每个在未来世界占有一席之地的人来说，《互联网上的间谍战》都是绝对必读之书，值得阅读、玩味、倾听。

温·施瓦陶

于佛罗里达州塞米诺尔

因特网由来

1969年大事迭出：内尔·阿姆斯特朗迈出人类在月球上的第一步；伍德斯托克音乐节上性自由和摇滚乐席卷安静的纽约小镇；纽约大都会棒球队成为历史上最年轻的美国职业棒球联赛冠军。不过，1969年之所以被载入史册，恐怕是因为发生了一件远比所有这些都更重要的事情；虽然在当时，它完全没有引起人们注意——1969年，因特网诞生了。

因特网源于一个简单的念头：连接美国各地几处科学实验室中的电脑。但人们很快就发觉，要搞成因特网，需要高层权要的支持。五角大楼通过高级研究计划局为因特网项目提供了资助。没过多久，第一个网络就出现了，被命名为高级研究计划局网[1]（又称阿帕网，即ARPANET）。不过，当时计算机联网的想法看上去有点离谱，理由十分充足：在1969年，计算机还是又大

① [illegible] http: //www.arpa.mil

又慢的机器，孤立运行，使用的语言五花八门，各个组成部件都很庞大，数据捣弄能力有限。当时，计算机唯一特别擅长的事就是出故障。每个按钮按下去都会弄得一群技术人员团团转。技术人员要能不修机器，得高兴坏了。处理阿波罗 11 号 3 位宇航员登月的信息就用了满满一栋楼的计算机。

加利福尼亚大学洛杉矶分校的两位计算机科学家罗伯特·泰勒和约瑟夫·C·R·利克里德在 60 年代中期提出，有朝一日计算机线路将不再封闭，而可以互通声气。之后不久，他们把这一理论付诸实践。1969 年 11 月 21 日，加利福尼亚大学圣巴巴拉分校、斯坦福研究所和犹他大学的计算机全部在加大洛杉矶分校联网，联网的计算机彼此可以传递信息。

把远程计算机相联，使它们能够互通信息，这在当时还只是空中楼阁。五角大楼虽然从 1966 年起就毫不犹豫地资助这一项目，但也不清楚怎样把它变成现实。凯迪·哈夫纳和马修·里昂合写的《因特网起源》一书记述了这期间流行的一个谣传：设计网络是为了对付核武器大决战。一旦这种危急局面出现，不论可能有多少苏联弹头在美国境内爆炸，网络需要继续运行。科学家们需要设计出节点，使得现在被分成一束束“数据包”——原始信息的片断或存储单元——的信息得以通过。每一个数据包经由不同的路径到达同一个目的地。核爆炸可能会摧毁各式各样的节点，但不会肃清整个网

络。因此只要还有通道，目的地本身仍然存在，数据包总能从另一条路径抵达目的地。今天的因特网也仍然是以这种方式工作的：你在发送电子信息或电子邮件时，永远不能确定数据包将从哪条路到达它们的目的地。

最早（很长时间里也是唯一）使用这些网络的是科学家。网络很快就成为他们争辩讨论科学、政治、文化等各种话题的论坛。应用网（USENET）诞生了，这是知识分子利用技术促进不同论坛内生动多样的讨论而建立的网络。这种论坛我们现在称作“新闻组”。不论什么网络都依旧是匿名管理的，它们各有各的名字、程序、结构和成员。

对我们来说，计算机内部通讯看起来可能很简单，但人类几乎用了四分之一世纪的时间，才克服重重困难发展出现在的网络。据 1995 年的一份研究报告，仅在北美洲就有 3000 多万台计算机上网。因特网协会提供的数字略有不同。协会在 1996 年 7 月声称，全球仅有 1300 万台计算机联网，但它进一步断言，网络新用户的数量将每年递增百分之三十。到世纪之交，全世界上网用户应当超过一亿。不管现在的确切数字是多少，注册上网的人比从前任何时候都多[①]。

---

① 据新华社 2000 年 2 月 16 日报道，截至 1999 年底，全球个人计算机总数达到 4.4 亿台，因特网使用者达到 2.59 亿。据预测，到 2005 年全球因特网用户将达到 7.65 亿。——译者

起初，受1969年时技术水平的局限，网络只能传输简短的文本。更糟糕的是，被传输的文本仍使用发送者计算机里的语言，而不是接收者计算机的语言。这样，没有哪台计算机能够搞清楚另一个网络的内容，收到的全是些不明不白的乱码。显然，最大的障碍是定义一种公共语言，以此为桥梁，跨越各自为政的网络之间的鸿沟。各种协议（Protocol）就这样应运而生。作为规范计算机之间数据传输的标准化程序，不论计算机规格、能力或操作系统有多大差别，这些协议一概通用。它们使一般性通讯成为可能，而且允许文本和数据的传输。

协议是因特网的基础建筑材料。最初有两项协议：传输控制协议（TCP）和因特网协议（IP），现在协议已超过100种。在高级研究计划局网最出风头的日子，由曾在加大洛杉矶分校念书的文特·瑟夫领头，因特网协会[①] 帮助网络管理器设立了它们自己的基本参数和协议，如电子邮件系统标准化[②] 等等。衍生出因特网的

---

① 创立于1992年，网址：http://www.isoc.org。

② 绝大多数地址都包括用户最后一个名字，后面缀以@，然后是为用户提供因特网连接的服务商或公司的名字。地址的最后一部分被称作"域"，表示用户所属的更大类别。如果用户是大学里的学生或教授，他/她的地址后面就可能是"edu"；如果是商业用户，就会是"com"，如果是军队，就是"mil"，政府则是"gov"，以此类推。在法国，用户地址最后一部分是"fr"，英国则是"uk"，芬兰是"fi"，俄罗斯是"ru"，如此等等。

网络在 1969 年横空出世，它不慌不忙地繁衍着后代。而且，早先也压根儿就没有多少计算机，有也是放在大公司和实验室里的笨重的庞然大物，它们黑色屏幕上闪烁的奇怪的绿色信号对任何没拿到计算机科学博士学位的人来说，大部分都是天书。光是记住各种命令就足以让我们中大多数人害头痛病。

80 年代初，计算机简单化进程初传喜讯。出现了凡夫俗子也能使用的个人计算机，如苹果的麦金托什（Macintosh）系列机。微软的创立者比尔·盖茨率先开发出针对美国国际商用机器公司（IBM）的计算机和兼容机应用的基本操作系统，如 MS—DOS 和后来的视窗图形界面。这些发展标志着微机的蓬勃兴起和因特网的第一个黄金时代，导致个人计算机降价和计算机威力陡增。

但直到 80 年代末，上网仍然很麻烦。协议不易理解和操作，连接不同区域的屏幕也无可救药地陈旧过时。因特网仍令用户望而生畏。

1989 年，因特网汪洋再涌新波：万维网（World Wide Web）诞生。发明者是当时在瑞士日内瓦欧洲核研究中心工作的蒂姆·伯纳斯—李。伯纳斯—李的初衷是为网上冲浪者提供比从前协议所提供的更容易的上网方式。一个“网址”可以由在更大的万维网框架内的一组服务器组成，其中所有内容能够在各组成部分之间迅速自由地移动。这个使传输既迅速又便捷的概念就被称作

“超文本”。比如说，用户看着屏幕上显示的目录，敲击一个特殊的字段，就可以直接被送到那里，毋需被迫再执行一堆复杂的协议。那些协议已经隐藏在万维网中。上网于是成了弹指般轻而易举之事，其结果实在令人惊喜：服务器甚至可以提供和其它服务器的超文本联接。按下一个键，在巴黎的用户几秒钟之内就能连接上一台日本的服务器，不仅如此，他还可以在全球作任意次数的停留。

1993年，马赛克（Mosaic）软件问世，这是最早出现在因特网上的万维网浏览器。因特网成为数百万用户日常生活的一部分。不久，又出现了用户更加容易掌握和使用的网景航海者（Netscape Navigator）软件程序，它们都是马克·安德雷森制作的。依靠这些软件，就连最初级的网上冲浪者也有能力充分利用因特网，这是前所未有之事。起初，每天都有数千份网景航海者程序被全球各地的用户免费下载，当时软件制作者遵循因特网先驱们的思想，不收取任何费用。这一来，不论公司、大学、数据库，还是个人用户，也不论在天涯抑或海角，都可以连上万维网，享受网上各种服务。而所有这一切，所需不过是一台计算机、一个调制解调器、一根电话线和由当地服务商提供的可拨入因特网的当地电话号码。以此为起点，通过安装有马赛克或网景航海者软件的计算机，用户可以自由自在地在网上冲浪，与全世界服务商连接，开销不过是本地电话费和每月给服务商

的一小笔上网服务费。

大网络最终衍生出大量小型网络，使各种用户都可以在超文本道路上旅行。所携带的虚拟货物或重要或琐碎；或冗长或古怪，都以电子形式在网上驰骋，种类之多堪与现实生活中的任何高速公路货运媲美。即时电子传输正在取代供应廉价威士忌酒的飞行和缓慢的跨陆旅程，各种数据以光速围绕地球运动，传输的信息数量之大闻所未闻。由此，出现了崭新的通讯观：一个人舒服地呆在自己家里，通过一台微机，可以无所不至。既然用户连接的大多数计算机都不大可能是美国政府储存黄金的诺克斯堡，那么不论对什么人，当然也不论对什么国家，几乎没有什么是不可企及的。对各国的谍报机构来说也是如此。大多数谍报机构早已开始在信息战争的幽暗世界里安营扎寨。

当前，计算机连接有两种不同的通讯方式。对一般老百姓，也就是我们大多数人来说，靠的是世界各地的电话公司。全球共有六亿多电话用户。通过绵延数以百万英里计的铜缆，电子传输相对快捷容易。不过，计算机专业用户，如科学家、公司和军队，所使用的连接手段就更高一筹。他们的接入路径所允许的信息传递速度非常高，你的因特网服务商首先与这些特殊的通讯设备连接，然后租用结构更大的底层窗口以导入订户。1995年以来，一些用户对综合服务数字网（ISDN，又译一线通）技术的兴趣日益高涨。通过高质量的铜电话线，数

据传输速度可以达到64千比特/秒[①]，这一速率足以传输声音和图像，并以更合理的速度下载文本和数据。就我们在电视上看惯的图像细节水平而言，综合服务数字网传输的图像要粗糙得多，即便用上图像压缩软件，也需要200万比特/秒的速度，才能达到电视那样的效果。速度更快的网络便应时而生，但它们可远远不像随处可见的家用铜线那么普及。超高速主干网络服务（VBNS）[②]是一个新出现的美国网络，它使用光缆和异步传输模式（ATM），连接速率可高达155兆比特/秒。异步传输模式技术直到最近才看到发展前途。但它还是有可能很快就会被速度更快的以太网（Ethernet）推下宝座。以太网的速度可以达到10亿比特/秒，恰好一个吉比特。

前景一片光明。作为计算机及其用户远程联络、反馈和获得信息的工具，因特网现在有能力传输声音和图像。但是目前铜制电话线路的传输速度还没有快到适合实时传输电影和电视节目的地步。各电话公司还在仓促

---

① 比特（bit）是数字信息的基本单位。构成英语字母表中的每个字母需要8比特。截止到1996年，一般说来，一根普通的铜制电话线每秒最多可输送28,800比特的信息。1996年以来，由于引入ADSL技术，同样一根线可以每秒传输800万比特的信息。

② 英文原文是：very high speed backbone network service。另有一种VBNS乃是very high bandwidth network service的首字母缩写，通译为超宽带网络服务。——译者

地准备着应付未来的变化，相信它们的命运取决于使用现有电话线上高速因特网的前景。电话上网使90年代的口号——信息高速公路（德语为Infobahn，意义相同）——成为现实。这种联系方式的好处是大多数家庭早就有电话，电话公司可以坐等多媒体计算机的光临，而且多媒体计算机也才刚刚开始慢慢进入市场。多媒体计算机最早出现在1996年春季，立刻被取了个“网络计算机”（NC）的绰号，顾名思义，当指它们软件的革新观念。这些计算机不再配备带程序的硬驱或光盘驱动器（CD—ROM），而是从所连接的网络存取程序。使用这种基本结构的计算机价格可以降低到500美元左右。类似的家电组合集电话、电视机和微机于一体，将能够即时通过因特网接收数字图像。这种未来系统（现在已经问世）与我们目前通常使用的系统其最大的区别在于高速传输的实用性。用户将能方便地借助于多媒体联接，与其它用户实时互动、玩游戏、订购电影和其它产品而且即时使用。电视将完全互动。

我在本书中力求尽可能少使用技术名词，但初次接触因特网的读者也能从中得到必需的知识，以便独自去作进一步探索。因此，在讨论现存各种站点、组织或服务时，我通常在脚注中给出相应的网址。所提供网址我均曾测试，读者应不难利用。至于连接因特网的特殊步骤，就像我说过的，你需要一台计算机、一个调制解调器、一根电话线和一位服务商。服务商数量正在急剧增

加，他们绝大多数都使用网景航海者或微软探险者软件，其中后者的市场份额正一天天扩大。尽管如此，像美国在线（American Online）和天才联机公司（Prodigy）等在线服务商也提供上网服务，但一般说来，满意程度差些（要慢一点，麻烦一点）。建议你在选择服务商时，最好转转看哪家有你喜欢的额外服务。这是一个竞争激烈的市场，找到合适的服务商应该不是什么难事。

对有心的读者，全书提供的各种网址（中央情报局的、美国总统的等等）当能提供特殊的调查途径。你对本书有何评论，可直接寄往我的电子邮件地址：jguisnel@calva.net

第一章 新型谍报机构

1994年2月21日，弗吉尼亚州阿灵顿市，魁北克街和内利·科提斯路交叉路口，一位驾驶加长美洲豹小汽车的小个子男人放慢车速，停了下来。他别无选择——前面有车挡道，绿灯亮了也不挪窝。事情透着点古怪。小个子坐在车里，厚镜片后面的一双眼睛惊愕地瞪大了。他留着小胡子，模样像会计师或者保险推销员。突然，不知打哪儿冒出几个人，把小个子猛地拉出车。小个子只觉得双手突然被几只强壮的胳膊拧到身后，抵住车盖，一下子就被铐上了。平时好喝两口的小个子看上去似乎更矮小了，一点没有大人物的派头。反间谍特工宣布逮捕原因时，他只想起一句话说："肯定搞错了，我，间谍?"

阿尔德里奇·艾米斯，美国中央情报局主管官员，中情局自二战结束时成立以来挖出的最大叛徒。他干了10年，致使几十名为中情局工作的俄罗斯特工被捕，其中10人后来被处死。柏林墙被推倒不过5年，艾米

斯就被判处无期徒刑，象征性地为美俄谍报机构之间的冷战画上了句号。旧债算清了。就算历史喜欢神秘地重演，“自由世界保卫者”和“共产主义侵略者”之间的战争永不会再以同一方式出现。

在冷战废墟上

1993年初夏，艾米斯被捕半年前，中情局局长詹姆斯·伍尔西和俄罗斯联邦安全局局长叶夫根尼·普里马科夫坐在了一起。他们一边喝着上好的葡萄酒，一边讨论双方新的合作。他们可谈的很多，譬如怎样打击据说正在俄边境贩卖核原料的黑手党，怎样才能最有效地遏制毒品走私和洗钱等等等等。这仅仅只是开始，俄罗斯最近还（当然是部分地）公布了60年代末以来俄罗斯支持各种恐怖组织活动的档案。

法国谍报机构——法国国外安全总局——的首脑克劳德·西尔伯灿，是第一位接待普里马科夫的西方谍报机构负责人。1992年一个阳光明媚的日子，在中央旅游局总部（位于巴黎蒙蒂埃大街，是个老式大院子，人们更熟悉它的绰号“水塘”），西尔伯灿会见了普里马科夫以及6名前克格勃高级官员。他事后描述了法国谍报领导人的感受——几个月后，美国谍报官员肯定也颇有同感。西尔伯灿写道：“奇怪得很，我们高层领导对他们毫无敌意，真不可思议，但的确没有恶感。我都简直

不相信自己这么写。但这些天来，我感到这地方笼罩着一种陌生而愉快的气氛，就像有时你和因长期争吵而很久没见面的亲戚在共进晚餐似的。空气中缭绕着某种怀旧感，一种一个时代宣告结束的感觉。历时久远的冲突走向尾声，似乎所有冰冷的汗水和流淌的鲜血都已被遗忘……”

苏维埃共产主义历时 70 年，为西方创建和发展大规模情报搜集机构等提供了非常方便的口实。当代西方谍报部门在经历战前纳粹崛起年代及战时与纳粹斗争的锤炼之后，转而倾全力对付共产主义国家。庞大的现代谍报机构就是在这一时期成立的，它们当中绝大多数至今仍保持着原来面目。美国中央情报局成立于 1945 年，是在战时情报搜集部门“战略服务处”的基础上组建的，任务是搜集个人情报（HUMINT）和执行秘密行动。1952 年，美国总统哈里·杜鲁门下令在马里兰州米德堡成立国家安全局，专门搜集技术情报（TECHINT），以补中情局之不足。如今，国家安全局雇员达 4 万人，年度经费预算达 35 亿美元。国家安全局深深埋在一大堆让人稀里糊涂的秘密里，它的公开情况就这么多[1]。

每当新成员加入国家安全局，他们得到的第一项告

[1] 国家安全局网址：http：//www.nsa.gov：8080，但意思不大。国家安全档案馆网址要有意思得多，可以从 http：//www.seas.gwu.edu/nsarchive/ 中看到一些解密文件。

诚就是要永远为国家安全局保密。编辑过地下黑客杂志《Phrack》的克里斯·乔根斯（又名血斧埃里克）为能公开国家安全局安全手册的大部分内容，感到欣喜若狂。在这份手册里，国家安全局安全负责人腓力浦·T·皮斯对新手强调了国家安全局的原则："本局从事工作之价值不可能具体用几元几角来估量，但毫无疑问，你在国家安全局所接触到的情报对美国国防至关重要。这些情报只有不为人知才可能派上用场，因此需要采取非常特殊的保护措施。各部门安全条例和规定已指出这种保护的特殊性，但整个国家安全局安全纲要内容更加广泛，其基本理念是：安全始于意识状态。纲要旨在增进对保护至关重要的国防情报的必要性的认识，强化安全意识，而不仅限于机械地遵守条例。有时，安全措施和手续会给个人造成不便，它们费时费力，间或还需要主动放弃某些习以为常的个人权利。其补偿则是在牢固的安全措施框架内，你在国家安全局的工作为美国国防和持续安全所作出的重大贡献。"

国家安全局以保卫国家安全为名，实际上窃听着电子或无线电波所能传输的一切信息。不管在地球什么地方，它都能侦听民用卫星通讯，给水下电缆安装窃听器，以及截取电磁波。国家安全局在电子情报项目（ELINT）下拥有船舶、飞机和电子谍报卫星。电子情报项目是技术情报项目（TECHINT）的一部分。国家安全局还和英国政府通讯总部以及澳大利亚安全情报组织合

作，委托它们在欧洲、中东和亚洲执行一些不太重要的任务。国家安全局使用的计算机根据其需要经过特别设计，是世界上威力最大的计算机。国家安全局是计算机设计师塞缪尔·克雷的第一位主顾。一直到现在，国家安全局也是克雷计算机最大的买主。简言之，国家安全局忙着控制全球电子经济，而其人手之众，做起这项工作来绰绰有余。

因特网自然已成为国家安全局偏爱的窃听目标。国家安全局实际上已经“绑架”了整个网络。如果没有哪家认真的公司信赖网络通讯，如果没有哪国政府上网发送敏感信息，原因就在于国家安全局的监控。国家安全局越来越密切地监视着美国各地的通讯，这些通讯绝大多数都在事主不曾察觉的情况下被国家安全局米德堡总部的情报网所过滤。地球上任何遥远角落里某个隐蔽的电子移动，都没有多大指望能逃脱国家安全局的注意。

事实证明，在前苏联和冷战时代，国家安全局是共产主义国家最无畏的监视者。铁幕沿着苏东国家边境垂落，西方无法派遣特工越过边境打入内部，这些都难不倒国家安全局。因为前苏联政府机关，包括军事机构和国营生产单位，还是不得不进行内部通讯。实际上，不论情报是通过电话、无线电或电报发出；不论它们经由地面还是空中的无线电波，抑或通过飞机或搜索太空的卫星雷达传递，国家安全局都一直在截听，以后也仍将如此。为达此目的，美国海军动用核潜艇在前苏联太平

洋沿海的一根海底电缆上安装了窃听装置，代号为“长春藤钟”。这是冷战时期最令人震惊的侦察行动之一。

新型谍报

许多国家的情报搜集机构都展开了新型谍报活动。尽管如此，美国国家安全局仍然是龙头老大，最接近的竞争对手在行动规模上也得甘拜下风。过去，唯有前苏联真正能与国家安全局一比高低，从事情报搜集和分析工作的前苏联特工曾经多达近35万。但正如他们所言，那都是老皇历了。

由于20世纪下半叶卓越的通讯技术革命，人们几乎可以找到所有情报源——不论是学术的、政治的、工业的、军事的，还是商业的。印刷品依然是传播信息的手段，但越来越多的文本正在通过电子方式传遍全球，速度快得令人难以置信。一本小说通过调制解调器几秒钟之内就能被送到另一台计算机里，信息一直在硬盘上不可见地积累着，一台普通的商用计算机可以存储成千上万页资料。全球数据库已经变成巨大的人类知识宝库，查询数据库信息的人数增加得特别迅速。这些新型信息库中，有些是公开的，任人浏览，不收费或收费甚低。另外一些则无论某些人肯出多少钱也不公开，内容保密。不消说，各国谍报机构所觊觎的正是这些数据库。为了强行进入这些数据库，谍报机构日益仰仗信息

黑客的帮助。

只认为各国谍报机构不再对信息革命无动于衷，那可远远没有充分表达出真实情形。恰恰相反，信息革命和这些谍报机构的日常工作已经息息相关。全球上网计算机已达到 3000 万台，行家里手可以逐渐而巧妙地深入虚拟世界的核心，看到大量令人吃惊的个人资料。国家安全局在过去四分之一世纪里一直在研究怎么做到这一点。

当然，老式谍报人员也还可以盼到某些执行秘密行动的光辉时刻，诸如去完成不可能完成的使命、到异国雾林深处进行生死搏斗——这些都是好莱坞惊险大片中的刺激场面。在这类富于娱乐性的跨国故事中，总有这么一个最基本的要素：电话窃听。1876 年格拉汉姆·贝尔率先开发出电子语言传输技术后没多久，窃听就成为警察的常规武器。今天，在日益宽广的信息公路上横行的信息盗贼，很大程度上仍然在利用同样的原理。这个陈旧的概念令我们关注之处，就在于它在截取各国境内的数字信息并对其进行专业分析方面的应用。对谍报机构来说，它特别感兴趣的首先是向传统边境概念提出挑战的信息转移。每日每夜，数以十亿计的比特漫游在通讯网络上，就好像跳动在一个巨大躯体的神经系统里的电子脉搏。电子不必在海关出示护照。在网络空间——正如小说家威廉·吉布森在《神经浪游者》（《Neuromancer》）一书中杜撰的数字网络通讯世界，所有边界

都是虚拟的。

前海军情报官员和肯塔基大学政治学系教授、华盛顿战略和国际研究中心助理研究员威廉·T·沃纳是世界上最熟悉现代谍报演变过程的学者之一。最近，在讨论导致美国防范新型谍报能力薄弱的新因素时，沃纳教授对新兴技术作了如下评论："电子'信息革命'使信息的发生、存储、转移和接收全部数字化，同时大大降低了数据控制和管理设备的规模、费用以及操作的复杂性。这些方面都和技术有关。过去，机密被记录在文件里，文件又被锁进保险箱里，窃取情报主要依赖古典的间谍技术，如动手偷盗具体方案或文件，行贿或者把掌管情报的人拉下水等等。这些技术都可能'留下蛛丝马迹'，有最后暴露的危险。而在'数字时代'，只需截取情报在被存储或被传输的某个点上的格式化数据，就能偷到情报。数字化信息管理技术同样培育出相对隐秘的电子窥探系统，利用这些系统可以不经许可地闯入受保护的数据库，或者非法截取数字化传输信号（国家安全局则在合法地这么做），如此等等。"

这一演变在谍报机构内部引起震荡，它与多年冷战发展出的令人生畏的技术设备及其警察式实用主义的应用格格不入。支持以全面监视公民社会为基础的秩序的人们难以接受这样的现实：相对透明的因特网几乎可以让任何人读到别人的电子邮件。人们不用费多大劲儿，就能够潜入他人的个人计算机，对肯定不该看的内容大

看特看。由此，我们最终清除了又一道隐私壁垒——在这个日渐萎缩的世界里，隐私壁垒已经所剩无几。

但是，道高一尺，魔高一丈。全球通讯网络在一片无政府主义的欢腾中迅速崛起，如影随形而来的是用以保卫我们个人自由的新工具。富有想象力的计算机科学家和数学家研制出各式各样的加密方法来保护特殊的网络通讯。这些虚拟锁一直在以光速免费发放给全球数以百万计的用户。而以美国国家安全局为首的各国谍报机构则一直企图抵御日益汹涌的加密潮流。处于青春期的网络王国，承受着风险巨大的成长的烦恼。

打击恐怖主义

冷战结束后，各国谍报机构不再一味窃听从前的对手，而把更多的时间和精力放在了别处。在法国，一系列新的问题受到关注。自 80 年代初以来，谍报机构把注意力集中到打击源于中东地区的恐怖主义。叙利亚、伊朗和利比亚都被牵扯进各种国际恐怖事件中。尤其在法国，1986 年发生恐怖主义袭击浪潮，1989 年 9 月 19 日发生法国联合航空运输公司 DC—10 客机爆炸案。1995 年 7 月 25 日，正值夏季旅游高峰，连结机场和欧洲迪斯尼乐园的巴黎公交铁道线发生炸弹爆炸。事隔仅一个月，8 月 27 日，巴黎主要旅游点香榭丽舍大街再次发生炸弹爆炸。

这是最早的两起袭击案件。从那时起到 1995 年 11 月，法国又发生一系列恐怖主义炸弹爆炸案，共计 8 人死亡，130 人受伤。阿尔及利亚恐怖组织伊斯兰武装组织领导人之一哈立德·凯卡尔于 1995 年 9 月 29 日被警察击毙。该组织在三座法国城市设有分部。为了追捕伊斯兰武装组织最高领导人，发现非法进入法国的伊斯兰武装组织全体成员，并摧毁恐怖主义者苦心经营的发号施令的关系网，法国警方把 40 年冷战里从追踪苏联特工中学到的一切全用上了：设藏身所、盯梢、调遣数十名擅长监听的反谍报专家参加行动。这些措施都是根据现实需要而采取的。由此，法国两大别动机构——法国国外安全总局和国家侦察中心——逐渐从搞冷战转向处理现代恐怖活动的紧急事件。两大机构不仅任意使用复杂的技术系统，还毫不犹豫地派遣特工到第一线单独行动。法国反间谍专家腓力浦·兰多特将军就是这样孤军作战，于 1994 年 8 月在苏丹抓获了臭名昭著的恐怖主义者豺狼卡洛斯。卡洛斯是一名委内瑞拉雇佣兵。15 年来，他一直为某些最好战的中东恐怖主义组织工作，狡猾地逃脱了各国谍报机构的追捕。最早在苏丹发现卡洛斯的看来是美国特工，可能是由美国国家安全局首先发难。接着，兰多特设法跟踪并抓获卡洛斯本人，拍下他的照片，然后把他转移到法国。至今卡洛斯还蹲在巴黎一所监狱里等候审判。不幸的是，巴黎系列爆炸案的悲剧一直持续到 1996 年 12 月 3 日，那天，一枚炸弹在

罗亚尔港站深层地铁列车内爆炸，致使4人死亡，126人受伤。

有些法国特工好比是踯躅在中东旷野的孤独的狼，他们嘴里咬着棍子面包，怀里揣着香烟，戴顶贝雷帽，在小巷游来荡去，对前苏联、美国中央情报局和以色列摩萨德特工打出蔑视的手势。但绝非所有法国特工都如此。事实上，十多年来，西方情报人员一直在截取和破译伊朗各使馆与德黑兰之间的通讯。1991年6月6日，伊朗前总理沙普尔·巴赫蒂亚尔在巴黎附近遭到暗杀。几天之后，反恐怖法官让—路易斯·布吕吉埃就得知，涉嫌杀手曾在伊朗驻巴黎使馆向基地打电话报告谋杀成功。此事被泄露给法国媒体，公众看到凶手与其德黑兰同僚的讲话内容，伊朗人也从此知道他们的通讯遭到窃听和破译，或用行家的话说，被解码了。

西方这场重大的情报战赢得十分轻巧，靠的压根儿不是密码专家的辛勤劳动。瑞典加密公司（Crypto AG）总经理汉斯·布尔赫说，伊朗用于一级机密通讯的密码系统是由该公司设计和出售的。公司同时把密匙副本送给瑞典谍报机构一套，后者又把副本的副本慷慨地送给了世界各地其它一些谍报机构。此事曝光后，1992年的大部分时间里布尔赫都蹲在伊朗监狱里。

80年代时，美国还没有在国内对付恐怖主义的经历，但它很快就着手发展反恐怖技术。1988年12月21日，美国遭到第一次打击：泛美航空公司747航班在苏

格兰洛克比上空因炸弹爆炸坠毁，机上人员全部遇难。随后，恐怖主义者袭击了世界贸易中心（1993年2月26日）、俄克拉何马市政府大楼（1995年）以及亚特兰大奥林匹克运动会会场（1996年）。这些恐怖事件的罪魁祸首有土生土长的美国人，也有外国人。显然，在这个非核时代，美国本土不再幸免于无目的的暴力犯罪活动。

现实要求美国人迅速转向在国内清剿恐怖主义。美国谍报机构因之一直为打击恐怖活动而奔忙，使尽一切手段。除国家安全局外，始建于1960年的美国国家侦察署也是针对这种重大需要而设立的政府机构。国家侦察署直到1992年才为外界所知，它负责追踪美国间谍卫星及卫星情报，每年花掉50亿美元窃听不利于美国的消息，以及时避免人员伤亡。国家侦察署后来觉得它可以不经行政授权就为所欲为，最近像谍报机构一样，惹出了很大麻烦。1996年2月，中情局局长约翰·M·多伊奇和国防部长威廉·J·佩里发现国家侦察署新总部的各项建设费用高得出奇，一些预算需求也很过头。他们当即采取重大措施，撤销了国家侦察署主任杰弗里·K·哈里斯及其助手吉米·D·希尔的职务。这件事发生前几天，参议院情报选择委员会主席阿伦·斯派特刚刚平息了不赞成国家侦察署的言论。

美国方式

恐怖活动使得美国损失惨重，但美国各情报机构仍然把大部分年度预算（1997年度达300亿美元）花在搜集经济情报方面，而不是用来打击恐怖主义。为外国私营公司利益打入美国公司的间谍，和采取措施系统地掠夺美国财富的国家，都是美国情报机构的头号打击目标。日本人在这方面表现出高超的能力：他们厚颜无耻地打入美国各行各业，偷窃、采购、贿赂，无所不施，不择手段地攫取情报；有时甚至向政府求助——通过外交邮袋传递情报。国家安全局分析员破译从三菱集团华盛顿办事处发往东京的加密文件后深感震惊，文件内容不是别的，而是中情局的逐日分类细帐，这是美国总统和国家安全顾问委员会才能看到的报告。几年前，日立集团打入美国国际商用机器公司领导层，通过日本驻旧金山领事馆把得到的情报（经日本外交密码加密）送回国内。德国和以色列也毫不逊色。德国曾因几度闯入专门从事银行内部计算机通讯的环球银行金融电信协会（SWIFT）网络而遭到美国指控。在以色列，摩萨德特工压制诸美国航空公司的投标，确保国营以色列飞机工业公司挤掉竞争者，获得价值达2000万美元的间谍飞机订单。

不过，美国应当把最佳经济谍报奖授予法国人。法

国国外安全总局特工这方面表现之出色无出其右，甚至因此在70年代引发了巴黎和华盛顿之间的外交纠纷。多年前，亚力山大·德·马朗什（绰号波尔托斯，即大仲马小说《三个火枪手》中又胖又壮的那位火枪手）执掌法国国外安全总局时，下令在著名美国公司的法国分公司中培植年轻优秀的工程师，充当法国国外安全总局特工。他们选择的公司均是一时之选：两家大型电子公司——美国国际商用机器公司和得克萨斯仪器公司，以及领导世界玻璃行业潮流的康宁玻璃制造公司。当时康宁玻璃制造公司正在研发前途无量的、为日后信息高速公路发展立下汗马功劳的光学纤维技术。此后数年间，法国特工还进入其它几家美国公司，它们多属竞争异常激烈的航空工业，如波音公司和达信贝尔直升机公司，当时这两家都正在准备制造具有直升机特点的混合型飞机V—22。法国还打入了最有创新精神的诺思罗普飞机公司，该公司以研制雷达探测不到的轰炸机出名，最早推出F—117和B—2型机。简而言之，法国对隐形技术专家全面出击，有时甚至在美国公司研究队伍里也成功地安插了鼹鼠。

慢慢地，法国工程师彻底成为他们所在公司的一分子，有的还级级晋升，实权在握。他们心照不宣，目的明确，即窃取商业和工业机密，令与其竞争的法国公司不需要付出巨额研发费用就可迅速获得技术优势。从慷慨大方的法国国外安全总局那里捞到好处的主要是贝尔

电子公司。当然了，贝尔矢口否认参与了任何这类谍报活动。

1988年，正值法国总统大选如火如荼之际，美国警醒了。一时还不清楚这些法国鼹鼠有没有受到内部谴责，是否从此扫地出门。总之，美国联邦调查局特工告诫许多法国特工说，联邦调查局对他们的所作所为已经了如指掌。消息反馈回去，巴黎陷入某种恐慌。某些政治要人被认定难辞其咎，因而大发雷霆。当时的法国国外安全总局局长弗朗科斯·梅尔梅将军于1989年3月28日被迫辞职，由克劳德·西尔伯灿接任。西尔伯灿上任伊始，就前往美国和中情局局长罗伯特·盖茨秘密谈判，为法国特工安排一条体面的退路。

从那时起，美国的态度变得咄咄逼人。比尔·克林顿第一次竞选总统时，便把打击外国谍报活动作为竞选口号。不过，上台之后，克林顿也让美国特工暗地里干起同样的勾当，优先利用谍报活动来壮大美国公司。克林顿政府带着一股子傲慢自大的劲儿和令人印象深刻的团结一致断定：他们别无选择。再说，他们也只是以其人之道还治其人之身。美国的战略和政治盟友同样也是美国的经济竞争对手，一如威廉·沃纳教授所说："美国的经济全球化不仅限于美国商业方式和商业运作的国际化，也展示了美国技术的优越，从而令所有人垂涎，并企图通过这样那样的方式把美国技术搞到手。绝大多数国家，不管是朋友还是敌人，都要么把美国技术当作发

展的跳板（例如法国、日本等国），要么和它‘挂钩’以求一己之生存（例如前苏联）。”

遏制洗钱

监视和分析通讯网络已经成为打击洗钱的基本手段。大多数工业化国家的谍报机构都下定决心斥巨资清查非法资金流动，为此动用了政治、司法和经济各方面的人力物力。美国金融犯罪执法网（FIN - SEN）和英国全国犯罪情报网（NCIN）共同建立了巨大的数据库，让缉毒人员、海关官员和银行管理机构互通声气，留心将大规模的可疑资金流动通报给当局。各国金融机构不同程度上都接受环球银行内联网（即环球银行金融电信协会网络）的监督，该网络监督之余，还坚持对大量数据进行金融分析。

但技术不是万能的，你还得对要找的东西心中有数，要能够估计到数目令人不安的贩毒款的动向。经济合作和发展组织（经合组织）的金融行动任务部就此提供了可靠的统计资料。该组织在1990年时估计说，全球毒品销售额每年达到1220亿美元，其中百分之五十到百分之七十五直接悄然回流到正常经济活动当中。不过，纵然能够搞到这样的情报，包括可赖以确认不正当交易的银行内部具体通讯情况，今天的西方情报机构有时仍然陷入非常微妙和复杂的境地。

今天，毒品走私犯不再是躲藏在铁幕之后的流窜之徒。他们利用移动电话相互联络，通过因特网传递加密信息，自由自在地旅行，在世界上最好的金融机构开设多重帐户。按照市场运行法则，他们快意地利用着这些威望素著、人人趋奉的殿堂，和其它顾客一样在里面作生意。他们貌似诚实的公民，却玩着肮脏的把戏。而谍报机构在这些银行遇到了很大困难，找不到办法对付狡猾的对手。正如经合组织金融行动任务部的报告所言："这些犯罪分子从事的是令人震惊的非法活动。他们必然要设法拥有这些金融机构能接受的流动资产或帐户。无疑，他们希望借此隐瞒与非法活动的关系。事实上，我们掌握的资料不足以对与洗钱有关的银行债务进行适当的评估。"报告又说："年复一年，情况越来越糟。根据 1996 年 5 月金融行动任务部估计，每年通过银行网络被洗'白'的非法资金达 3000 亿美元。1997 年金融行动任务部的'近忧'是数字现金的投入使用，数字现金允许人们进行匿名安全交易，而且对守法公民和骗子恶棍一视同仁。"

第二章 网络武士初出江湖

约翰·派里·巴劳一头长发，下巴上蓄着整齐的小胡子，看上去像个既随和又讲求实际的家伙。他靠给“感恩逝者”（The Grateful Dead）等乐队写歌过着优裕的日子，如今在怀俄明州萨布莱特县买下了一家养牛场。1989年年底，巴劳听从一位音乐家朋友的建议，上网冲浪，头一回访问热心的网虫们常去的“全球电子联接”网站（WELL：Whole Earth 'Lectronic Link），也有生以来第一次和警察打上了交道。

电子边疆基金会参战

1990年1月15日，美国电话电报公司（AT&T）在美国东北部地区的电话网发生严重运行困难。巴劳和其他人一样，以为可能有黑客闯入了美国电话电报公司的计算机。他万万没有想到，在逐渐展开的调查中，他自己成了嫌疑犯。联邦调查局怀疑他是新普罗米修斯网

（NuPrometheus）成员。新普罗米修斯网曾非法获得并发布了苹果麦金托什（Macintosh）计算机使用的只读存储器（ROM）上的许多源代码。

1990年4月，联邦调查局特工、来自岩石泉的牲畜偷盗专家理查德·拜克斯特和巴劳进行了长达三个小时的干巴巴的谈话。巴劳由此确信联邦调查局正处在惊惶失措的状态，在这些执法者眼里，他的基本权利之一——自由通讯权——被划上一个大大的问号。巴劳说："我在谈话过程中认识到，我正在目睹整个美国执法结构的缩影。特工拜克斯特不是唯一搞不清楚数据犯罪的法律、技术和抽象性质的执法者。在网上《哈泼斯》杂志的计算机和自由论坛里，我遇到一些年轻黑客，他们最近遭到了谍报机构的搜捕。拜克斯特的思想斗争使我大致明白了这一系列搜捕行动是怎么回事。我料想这可能是政府惶惑症大发作的开始，每个人的自由都将因此陷入危险之中。[①]"

巴劳把因特网当作倾吐忧虑的理想场所，他在网上大声疾呼，措词激烈，发自肺腑。在蓓蕾初绽的网络空间，他的抗议引起另一位富翁迈克尔·卡波尔的由衷共鸣。卡波尔靠写软件程序起家，不到30岁就当上百万富翁。1981年，他创立了莲花计算机发展公司（Lo-

① 巴劳：《电子边疆基金会简史》，可通过USENET（comp. org. eff. news）查找到。

tus)，于1983年以低价售出（在新业主经营下，10年之后莲花公司在网络通讯软件市场所占份额达百分之三十四，紧随其后的竞争对手微软公司只争夺到百分之十二的份额。1995年，基于其支配性的市场优势，国际商用机器公司以令人惊羡的33亿美元价格买下了莲花计算机发展公司)。到1989年，卡波尔已经半退休，大部分时间都用来上网，联邦调查局也曾光顾过他在马萨诸塞州的家宅，所以巴劳的言论深得其心。据1994年6月号的《在线》（《Wired》）杂志报道说，两人相见恨晚，“一谈就是三个小时，讨论了自觉性、网络和对公民自由的威胁。两人都相信他们站在了网络所孕育的伟大事业的门槛上，网线串起人类，势将重建文明。面对面会谈后，他们通过电子邮件继续交谈，一致认为他们应当携手干番事业。但是干什么事业呢?”

两人很快就有了主意：建立一个论坛。内容都要和网上自由有关。这就是电子边疆基金会（EFF：Electronic Frontier Foundation)。现在这个论坛已经成为因特网民意的代言机构之一，美国当局必须面对的对话者。

卡波尔和巴劳鼓吹言论自由的立场，使他俩在大力倡导信息高速公路的美国副总统阿·戈尔那里出了名。两人甚至在1990年宣布电子边疆基金会成立时，就预告了他们的既定目标。他们在《跨越电子边疆》一文中说：“以目前情形而论，网络空间可谓边疆地区，人口只是寥寥几位吃苦耐劳的技术专家。他们能够忍受原始

的计算机界面的严峻面孔、相互排斥的通讯协议、产权障碍、文化和法律的模糊不清以及有用的地图或暗语的普遍匮缺。当然，特性、表达、认同、运动和内容等以具体表象为基础的旧概念不再能简单地应用到这个虚拟世界里。这个新世界的主权也没有得到很好的界定。大型机构组织跑马圈地，占山为王；而绝大多数真正的网络土著都是孤独的单干户，间或还有反社会倾向。因此，不论对亡命之徒还是治安警察来说，网络空间都称得上是完美的孳生地。"

由于电子边疆基金会的诞生，和联邦安全机构有关的诉讼案冲出了樊篱。这些案例先前绝大多数都为媒体所忽视。据迈克·葛德温在《电子边疆基金会和虚拟社区》一文中说，"传媒不报道这些故事是因为他们不知道，或者至少是不理解问题所在。"

电子边疆基金会的创立者家财万贯，他们为这一事业投入了必要的人力、物力和财力，并聘请一流律师为被联邦官员追捕的黑客辩护。斯蒂芬·杰克逊案即是一例。这是电子边疆基金会创立伊始采取的公开行动之一。杰克逊是位信息游戏生产商，美国政府指控他的游戏"网络朋客"（Cyberpunk）会鼓励信息黑客行为。为查禁"网络朋客"游戏，谍报机构没收了杰克逊的所有资料。1990 年 5 月 8 日，美国警方展开代号为"太阳魔鬼"的大规模行动，从 14 座城市的青少年手中收缴了 40 台计算机和 2．3 万张软盘。警方行动当即激怒了电

子边疆基金会。

电子边疆基金会还帮助过克莱格·内多尔夫。这位聪明的年青人被控在一份名叫《Phrack》的深受黑客欢迎的网上杂志上发表了一家电话公司的部分内部文件，竟因此被判60年监禁和12万美元的罚款。多亏电子边疆基金会律师的帮忙，内多尔夫才重获自由——在他提出上诉4天之后，芝加哥联邦法庭撤销了这个案子。

电子边疆基金会和“计算机专业人员承担社会责任”协会很快就结成自由阵线，合力抵御试图控制电子信息流动的势力。他们的战场就在网上，而美国宪法则是他们最有力的武器。美国宪法第一修正案有云：“国会不得制定法律……剥夺言论自由、或舆论自由、或人民和平聚会的权利、以及呈请政府洗雪冤情的权利。”他们把第一修正案既当矛，又当盾，攻守两便，进退有据。

他们最后的保护神则是宪法第四修正案。第四修正案特别指出：无适当理由不得颁发搜查令和逮捕状，搜查令和逮捕状上需明确指出所要没收的物品和搜查地点。虽然没收计算机和存储着数以十亿比特信息计的硬盘已成为警方的家常便饭，更不必说他们窃听电话和网上交谈的频繁程度，电子边疆基金会及其伙伴相信这些做法明显侵犯了美国公民的权利。

电子边疆基金会的律师们所采取的游击战略收到震撼人心的效果，并导致信息自由法的出台。根据信息自

由法，人们可以了解任何与被调查嫌疑人直接相关的政府资料。早在电子边疆基金会创立之初，这些律师就查明：几年来，美国情报机构一直在暗中监视因特网服务器的生产情况。这一消息的披露，为网络空间敲响了警醒的钟声。

解码器与侵犯个人自由

最吵吵嚷嚷地强调法律和秩序的人中，有许多对因特网抱怀疑态度。网络空间早已成为人们聚会和交往的场所。说句题外的话，甚至越来越多的经济交易也在这里进行。网络空间看上去太无法控制，太无政府主义，技术性太强，太标新立异；而且坦率地说，还充满太多的变数。警察不能够合法地监视和惩罚网上异端。

结果呢，甚至连警方也在探索新的边疆。他们试图铺筑网上车行道，给无论哪里的网上冲浪者都划下标识线。现行执法体系无法容忍对电子通讯放任自流、不予监督的想法。在西方民主社会里，普通公民所能指望保留的隐私本来就只有那么一点。然而，普通公民维护隐私的愿望竟使得（以保护公民为己任）的执法人员举步维艰……这中间含有莫大讽刺。但按警察的逻辑就没什么可笑的了：警察的愿望是服务和保护，为此他们将使用一切必需的手段。

在美国乃至全世界，执法机关滥用权力的现象有着

悠久的历史。我们付邮的信件在收信人收到之前就已被非法拆阅，我们拨打的电话会被政府好奇地窃听。这类非法行为很难被查出，也几乎不可能得到证实，从而也就大多都得不到惩罚。

这种事情每天都在世界各民主国家上演着。对宁愿忘却这些的人们，1995年春败露的西班牙电话窃听案不啻是一剂有效的清醒剂——西班牙谍报机构非法窃听社会名流的移动电话，甚至窃听到西班牙国王胡安·卡洛斯头上！当然，西班牙国防情报中心是越权行事，但这一类逾越法律的做法长期以来早已是不成文的规矩。

恶念往往轻而易举就能实现，就好比做细菌培养时，用的有盖玻璃碟子上的细菌那样容易繁殖。美国前总统乔治·布什批准过国家安全局提出的一项可恨的计划，即在美国制造的每台电话或计算机上增加一个叫作解码器的芯片装置，这个芯片将大大方便当局窃听和截取私人通讯。布什卸任后，克林顿也热心支持这个想法。

解码器的构想很简单。技术进步和非法窃听使人们越来越难以进行私下交谈。有鉴于此，越来越多的平民百姓开始给自己的交谈和信函加密。普通人使用的密码术（详见第三章）又增加了执法工作的难度———旦真的发生犯罪事件，执法者更难弄到检察官所需要的情况。这样到了1987年，在美国国家标准和技术研究所敦促下，在凯普斯通计算机安全法计划范围内，国家安

全局针对新出现的监视难题，设计出一套被列为绝密的监控办法。

个人用户仍将继续保有电话、计算机或传真通讯的加密权利。从前，这类加密可以通过软件程序完成，政府发明的新办法则是在电话或计算机内增加一个新部件，即专门给通讯加密的微处理器。这种后来被称作解码器的微处理器将只有一种型号，安装它将使机器造价增加一千美元左右。解码器（规格保密）制造商是经常为五角大楼工作的政府承包商（VLSU 和 Mycotronx），他们将把解码器卖给硬件制造商。这样，消费者或公司花钱购买解码器后，就能够放心通讯，而不必担忧遭到干扰或窃听。

然而，国家安全局还暗中藏了一张王牌。每个植入神奇的解码器的装置在工厂都被配了两套密匙。作为第三方密匙保管系统的一部分，两套密匙不仅存放在用户锃亮的新机器里，而且经过复制，悬挂在两个互不相干的独立实体（政府从未说清是什么实体）的钥匙链上。两个独立实体根据第三方密匙保管系统对复制的密匙进行编档保存，它们只有在一种情况下可以交出密匙：即调查密匙持有者的犯罪行为时。如果这类调查需要用到密匙，就可以启动严格的解密程序了[①]。

---

① 有兴趣的读者可以在多萝西·邓宁的主页上看到更多的资料。邓宁的网址：http：//guru.cosc.georgetown.edu/denning/crypto

1993年4月16日，克林顿政府宣布了解码器计划，这仿佛在网络空间引爆了一亿吨梯恩梯炸药。对因特网用户来说，解码器不折不扣是国家安全局的点子。而政府却信誓旦旦地保证说，两套密匙依旧是安全的、保险的，谍报机构鞭长莫及，这就让绝大多数人都不能不反胃了。虽然国家安全局只是最粗略地勾勒出整个方案，虽然它正计划着用新软件“磕头虫”（Skipjack）来运行解码器，但这些全都无济于改变网民的心态。而且“磕头虫”软件和下章谈到的PGP加密程序大不相同。PGP的说明书全部公开，因而独立分析员能够对其详加剖析，以寻找其潜在弱点。而“磕头虫”的全部产品说明都属于绝密，人们无从分析它。这使得许多人怀疑国家安全局能够毫无困难地破解“磕头虫”，就像破解其它业经国家安全局许可进行商业销售的软件一样。对希望保密的消费者来说，所有这些软件在不同程度上都是废物，因为国家安全局的超级计算机能够轻而易举地“看穿”它们。

解码器计划大大侵犯了通讯自由和通讯秘密。对旁观者来说，这和白昼一样昭彰。白宫宣布解码器计划之前，国家安全局技术人员就和制造商及政府一道为此秘密工作了四年。此计划宣布前一年，国家安全局就和制造商私下签署了生产合同。而政府却还在言之凿凿地声称，国家安全局业已证实，没有司法许可，解码器的“后门”就不可能被打开。对此，网上报以一片嗤笑。

解码器计划正式宣布之日，即是第一次网络战争爆发之时。

第一次网络战争

在电子边疆基金会的积极努力下，解码器计划就像野火一样传遍网络空间。在电子边疆基金会看来，毫无疑问，解码器使每个人的通讯都受到威胁。反对解码器的社会层面之广是史无前例的。网上传播着一份抗议总统解码器计划的请愿书，很快就收集到成千上万个签名，其中包括所有网络缔造者及众多各界知名人士的签名。

反对解码器的人担心两个问题。密匙被存放在正式独立于政府的实体里，可谓荒谬至极。没人相信机密会得到郑重其事的保障，更没有几个人相信谍报机构找不出办法弄到密匙。这些是最常见的观点，但还远远不是最刺耳的抨击。另一些反对者认为，磕头虫软件完全是个不确定的未知数。还有些人觉得负责所谓安全问题的微处理器已经过时，运行之慢令人沮丧。

这是网络创立以来形成的最大的反对联盟，成员既有网络的“普通”用户，也有在网际旅行的所有颠覆分子——黑客和“网络朋客”之流，后者包括“加密无政府主义者”和“加密朋客”。他们全都好像看见解码器如同一块红色披肩正在他们眼前上下翻飞。不仅是他

们，计算机制造商也不开心。他们担忧政府把这种僵硬、昂贵的密码系统强加于人的企图会惹恼顾客；更何况 PGP 加密程序仍然在使用，它比“磕头虫”更灵活，更强大，更安全，而且还不要钱。计算机制造商们还担心出口产品时，外国买主可能不乐意由美国政府掌管能打开他们资讯的密匙。这一来，各派人马同仇敌忾，结成联盟。《时代》杂志就美国人对解码器的态度进行民意测验（很多被询问的人都还不明白怎么回事），结果百分之七十的人说，对他们来讲，和执法机构掌握窃听罪犯通讯的手段相比，保护隐私更加重要。

奇怪的是，因特网为谍报机构和抗议分子提供了以新的形式相互搦战的论坛。在各个新闻组里，赞成派和反对派都展开了活跃的论战。这还不算完，双方还举行了面对面谈判。对立双方通过这种成熟的相互交流，摆脱了各自偏执和不信任的积习，打了几次惊人的遭遇战。尤其是在 1994 年 2 月 2 日，促成了电子边疆基金会和国家安全局与联邦调查局代表的会晤。关于这次会晤的详尽报告后来在网上广为流传。报告向捍卫通讯自由的人们详细叙述了国家安全局所提要求及关键问题——解码器装置中的密码恢复程序——的具体细节。妙的是，谍报机构代表澄清了一个事实，那就是他们无需一纸司法公文就可以申领密匙——他们只要填张表担保自己有法律授权就成，司法部门的许可证可以以后再补办。在执法者看来，这样做无可厚非，因为，就像他们

声称的那样，他们只是想抓坏人，抓那些受到诱惑，利用加密通讯来达到邪恶目的的美国人。

这么做等于可以不先经查实和法律裁定，就进行搜查和逮捕，从而严重悖离了现行法律。但最终，甚至连这一点也无关紧要。在网上大辩论中，一位网络教皇级的人物（巴劳）指出："在某些权限不清、显然反复无常的法律当局辖治下，他们还将能够旁听我们的电话，阅读我们的电子邮件，而不必在后院里重新接线。他们将压根儿不需要任何许可来监听国际长途。如果这会发展成一场战争，我宁愿和现在这个政府打，也不愿意和我们那时可能面对的政府打。那时的日子就艰难了。嘿，我以前从不偏执，我一直认为大多数政府都太无能，一个好点子连从工间休息到下班时间那么久都不能维持不变。但现在美利坚合众国政府使我十分紧张不安。"记者布洛克·N·米克斯补充说："利害相抵吗？是的。彻底剥夺我的权利吗，休想。"

世事变幻如白云苍狗，没有什么事不可能发生。所以也就有了下面的事情：正值大辩论白热化之际，网民圣经、世界上最富创造性和原创力的出版物之一——《在线》杂志，邀请国家安全局撰稿，给了国家安全局首席法律顾问斯图瓦特·A·贝克整整三页篇幅来说明谍报机构的观点，又用一整页刊登了作者穿白衬衫、打领带、发际渐秃的照片。这之前，《在线》出版商简·麦克考菲曾形容自己是在"以洗礼派牧师向魔鬼献上周日布

道坛的全部热情”向贝克约稿；因此贝克在文章开头先用滑稽的笔调向麦克考菲致意。接着，贝克尽其所能地驳斥了关于解码器的“神话”。当然了，贝克声称国家安全局的唯一兴趣是追捕罪犯，不让“强盗们”从不可破解的加密软件中获得不公平的优势。他说，这些加密软件所提供的是“浪漫的高科技无政府主义”，“推翻未来某个暴君的游击队员也许会腰缠子弹带，手提袖珍保护装置，通过网络传递经过 PGP 程序加密的信息。但仅仅为了维系这么一个穿凿的设想，就向儿童色情犯和其他罪犯提供保护，我们社会是无法承受其后果的。”

想让犯罪分子放弃非法却高度有效的秘密通讯手段，改用剥夺他们隐私的昂贵的电话和计算机，这起码是不太可能的。不仅如此，相信所有人都愿意为所谓的改善法治而牺牲个人隐私权，这未免太过自说自话。有的罪犯住在公寓里，难道为了这个缘故，所有公民就应该在附近办事时留下复制钥匙，只凭当局一句保证说没有人会趁他们外出时拜访他们……除非得到法官批准？每年都有人成为枪下亡魂，但公民携带武器的权利仍然固若金汤，偏偏私下交谈的权利却受到了严重威胁。

更有甚者，围绕这个问题的争论还比不上政府所隐瞒的事实更令人关注。多年来，谍报机构一直不经任何司法授权就在侵犯公民隐私。儿童色情犯和毒品走私犯一直在被谍报机构用作侵犯公民权利的借口，而他们真正感兴趣的是窃听整个社会，包括政治家、艺术家、记

者、商人，而绝不仅仅是犯罪分子。虽然政府坚持说用不用解码器全凭自愿，但没有人相信政府的话。事实上，几年之后，1995年8月16日，电子保密信息中心透露说，国家安全局、联邦调查局和司法部曾拟定一份秘密文件并于1993年2月送交国家安全委员会。文件表明，三家机构计划让所有打算为通讯加密的人都使用解码器。解码器的热心鼓吹者处处露出破绽，电子边疆基金会就此大张挞伐，终于令解码器石沉海底。

1994年7月20日，美国副总统阿·戈尔在致反对解码器的国会议员玛丽亚·坎特威尔的信中宣布，白宫放弃原有主张，向解码器反对者让步。白宫并没有放弃解码器的念头，但他们表示解码器不再是非装不可。事实上，只有政府自己使用解码器。这一来，这个装置的寿命就和一台新复印机差不多。这就解决了个人隐私问题吗？非也非也。公开宣布还公民以个人和商业生活中的自由通讯权利是一回事，相信网络空间的好日子会风平浪静直到永远又完全是另一回事。企图管制持续增长的电子流动的势力注定还会卷土重来，而且会包装得更加吸引人，更加孜孜以求通过某种方式驾驭蓬勃发展的网络空间。解码器被判死刑数日后，几位政府官员写出一份冗长的有关报告，表现出比国家安全局代言人斯图瓦特·贝克在1994年9月时更理性更务实的态度。报告写道："在生产和使用信息安保的商界和学术界，以及一般公众中间，对以国防安全目的为主导的保密和安全政

策的关注倍增……以前，人们主张控制加密技术的传播和使用，是把它当作一个重点对外的国家安全问题，动机是保持美国相对于其他国家的科技领先地位。如今，国内政策日益注重打击犯罪和恐怖主义，加密技术的传播和使用也作为一个国内安全执法问题日益突出。加密技术在国外已得到更加广泛地运用，恐怖主义者和发展中国家都在利用它，使得美国更加难以识别情报。在美国国内，加密技术正日益被渲染成对国内安全（公共安全）的威胁和执法的障碍——假如恐怖主义者或犯罪分子对其唾手可得的话。人们也日益认识到，加密技术可能会被误用和滥用，例如被牢骚满腹的雇员用来破坏雇主的数据库……优秀的加密产品被犯罪分子和恐怖主义者大量使用会对社会治安和国家安全构成极其严重的威胁。加密威胁的本质在于便于掌握和使用的优质加密产品能够严重妨碍执法部门和反谍报机构进行电子侦察，而这往往是后者在依法完成任务，履行责任时所必须做到的。”

很难再把利害关系说得更清楚了。电子边疆基金会很快就醒悟到，他们虽然赢得解码器之战，但政府压根儿就不准备偃旗息鼓，对加密问题放任自流。政府反攻必定是残酷的。

国家安全局和联邦调查局虽然在解码器问题上吃了败仗，但到 1994 年 10 月，却出人意外地获得了数字电话法案的胜利。该法案规定，公司在设立非常难于窃听

的数字电话网时，必须为政府机构留出进入电话网的路径，以便政府机构能够截听。因此，解码器计划虽然总的说来流产了，其部分内容却在另辟蹊径成为法律。

在美国和其它地方，通讯技术的突飞猛进令警方一方面要努力利用这些技术，同时又得苦心积虑不让这些技术为对手所用。警方的处境为之改变。现在，他们必须关心的不再只是电话，还有因特网通讯。可能的通讯方式正不断增多，要维持窃听手段，这再也不会像摆弄电话窃听器那么简单。警察既要注意获取家庭和办公场所的信息源，又得破解保护这些信息源的密码。而且，这还不是结局。

性和网络警察

《正当通讯法》是新面世的一项反网络措施。它是由参议员詹姆斯·J·埃克森和参议员斯拉德·乔顿发起的。法案看来把联邦通讯委员会的权限从广播电视领域扩展到了广袤的网络空间新世界，为保护网上冲浪者，防止猥亵、淫秽、性骚扰和侵犯个人自由现象的蔓延制定了若干规定。法案作为电子通讯法的修正案，规定网上内容的供应商和内容所流经网络（例如电话公司、因特网公司、BBS（电子布告栏系统）企业、计算机服务公司、美国在线和天才联机公司（Prodigy）都有责任杜绝粗鄙的内容。

这一限制性很强的法律，不管措辞多么谨慎，还是正式授权给执法部门监视和窃听网上众多涉嫌撰写或推销色情文学者、儿童色情犯、兽行的人、有食粪癖的人以及其他恋物狂。对那些兽行狂或最新式的性虐待狂和性受虐狂来说，因特网不啻是完美的探宝天堂。何止于此，因特网为所有网民——修正主义者和新纳粹、酷刑和死刑的狂热支持者、基督教极端派教徒、伊斯兰原教旨主义者、各方各派的民兵、其他各种反常的偏执狂——都提供了自由憩息之地。和那些饲养仓鼠或栽培玫瑰的人一样，他们也都有专门满足自己兴趣的新闻组。1995 年 4 月 19 日俄克拉何马市爆炸案后，就连最没经验的网上冲浪者也能撞见新闻组里有个别疯狂的专家。这些专家声称爆炸案不能算真正的成功——毕竟只炸死了 168 人，炸伤 500 多人；他们并且提供了更具破坏性的炸弹配方和各种能达到诸如此类疯狂结果的特殊方法。

不过，因特网首先是用于发送电子邮件，兼以查询原文和科技档案，召开电子会议，进行网上交谈，以及创立新闻组，但新闻组并不总是由组织者主持。那么，美国政府为什么要限制公民以电子形式聚会和发言的权利呢？《正当通讯法》的支持者回答说：因为儿童也越来越频繁地上网冲浪，有必要采取措施防止孩子按下手中的小老鼠（鼠标器），却看到儿童不宜的东西；也有必要防范街头恶棍式的网络流氓接近孩子。可是，该在

哪里划下禁入线？1994年7月，田纳西州一陪审团判处加利福尼亚州米尔皮塔斯一对年轻夫妇——罗伯特·托马斯和卡莲·托马斯有罪。罪名是通过“业余行动”BBS销售色情照片。此案审理中我们得知，按加利福尼亚州法在BBS硬盘上存储色情图片是完全合法的，但田纳西州法则禁止打开这类图片。而且，虽然当地居民是自愿付费下载这类图片，田纳西州法律仍有权搜捕和惩戒托马斯夫妇。正所谓天网恢恢。

对以《正当通讯法》形式出现的愚民政策回潮，电子边疆基金会和其它组织一道奋起反击。抗议活动组织者之一大卫·约翰森，于1995年2月10日在电子边疆基金会网址上解释道：“我们相信，决策者应当考虑到网络用户拒收令人厌恶的内容的能力。将来也许会更多地利用信息标识和首标来避免接收不需要的资料和指导孩子们使用因特网。与此同时，我们相信把‘传输’令人讨厌的材料当成犯罪纯粹是个糟而又糟的主意，特别是当‘传输者’属被动的一方，并没有监督所‘传输’内容的时候。”不妨把约翰森的观点看成是问题的一个方面。

民主和科技中心的杰里·伯曼曾试图建立一个《反正当通讯法》组织。他相信，任何管制网络的图谋都是对最基本的民主自由的侵犯；因特网有能力自己管理自己。他说：“人们总是认为，政府控制大众传媒内容，这对避免儿童接触赤裸裸的性内容，和防止听众/观众

不知不觉间接触到可能被认为是极其令人作呕的材料，是至关重要的。历史上，保护儿童的选择，就一直与禁止政府新闻检查的第一修正案相抵触。现在，国会要管制新的互动媒体，关键在于国会必须明白互动媒体和大众媒体是有差异的。互动媒体的能力和灵活性为父母控制子女所接触的内容提供了独一无二的机会，同时成年人想要的信息流仍然可以畅通无阻。所以，要达到保护儿童的目的，根本不需要政府的控制管理。”绝大多数公民自由保护组织、多家报纸、制造商（如苹果计算机）等等都赞成和支持伯曼的观点。

论争日趋激烈。这时网络却自行找到了解决根本问题的办法。这一点利害关系极大，因为绝大多数与网络有关的企业和用户都想尽可能摆脱政府管制，力求按照不成文的规定进行在线贸易和享受网上娱乐，使用技术手段来控制无拘无束的电子自由所造成的实际问题。以此为宗旨，出现了一系列公约，合称为《因特网内容选择宣言》。这些公约使成年人可以自己给家中浏览器编制程序，忽略带有儿童不宜标识的内容。娱乐软件顾问委员会一向都非常积极地在给各种软件按适宜程度分等定级，许多公司也在营销用来控制上网的软件。这些软件的工作方式都相同。每种软件都包括一批定期更新的网站名单，并禁止机器登录这些网址。不过，这种过滤软件开发商对“黑”名单严格保密，用户搞不清楚哪些网址被禁止登录，特别是每天都有一批新网址产生。看

来，新闻审查又一次露出了它的丑陋面目，这回是打着反对色情的花旗子，把新的道德教条偷偷塞给老百姓。“网络阿姨”（Cybersitter）丑闻为个中危险作了清楚的注脚。

“网络阿姨”的开发者是硬橡木软件公司[①]老板布里安·麦尔伯恩。和Spyglass公司制作的“网络保姆”[②]（Netnanny）与“冲浪观察”[③]（Surfwatch），以及微软公司制作的“网络巡逻”[④]（Cyberpatrol）等类似软件一样，“网络阿姨”也是用于“保护儿童”的。但事情远没有这么简单。德克兰·麦克库劳和布洛克·米克斯在在线杂志《网线快讯》[⑤]（Cyberwire Dispatch）上披露了这些过滤程序的开发秘闻。他们的发现令人惊愕：这些过滤程序不仅阻止人们登录色情新闻组和色情网站，还有阴暗的一面。仔细研究一下被禁止登录的网站的具体范围就会发现，这些审查官查禁的远不仅仅是色情站点。事实上，有些过滤程序还禁止登录讨论男女同性恋问题或女权运动的新闻组，《在线》杂志的电子版《热线》（Hotwired）连整个“域”[⑥]都被限制登录。甚至连一个安全

---

① www.solidoak.com/index.htm

② www.netnanny.com/netnanny

③ www.surfwatch.com/

④ www.cyberpatrol.com

⑤ www.cyberwerks.com/cyberwire/

⑥ 为便于管理，因特网用户按域划分。

使用烟花爆竹的专题网址都被查禁了。

这些审查官们每天都会发现他们可以谴责和封锁的新站点，并以此为乐。而当麦克库劳和米克斯这样的记者开始报道他们的所作所为，使得他们的饭碗有被砸破之虞时，这些审查官们便反扑了。麦克库劳和米克斯的文章发表数日后，布里安·麦尔伯恩就向两位作者发出充满威胁的电子邮件。麦尔伯恩写道："我公司所筛选档案受到版权保护并经过加密。你们公布其中部分内容惹出了种种麻烦。你们公布的部分是资源码的片断，令我们的竞争对手得以洞察我们过滤引擎的工作情况，从而降低了我们产品的价值……我们将谋求根据版权法（《美国法典》第 17 部分第 503 条（a））起诉你们犯有重罪，并准备材料连同罪状一起呈交给联邦调查局。"

"网络阿姨"除封锁了"男女同性恋权利"、"全国妇女组织"、同性恋讨论组及女权主义讨论组一类的站点之外，也把胆敢讨论新闻审查或反对使用过滤程序的站点列入另类，令"家庭焦点"之类的组织颇为满意，将之推荐给其成员。而遭到查封的网址的创立者和经营者甚至不知道自己已经被列入了网络黑名单。查禁者的行动不受任何惩罚，但合法性却大可怀疑。像 alt . feminism , alt . feminism . individualism , soc . feminism , clari . news . women , soc . support . pregnancy . loss , alt . homosexual . lesbian，soc.support.fat - acceptance 这样一些对少数群体的精神健康为害极微的讨论组也全被"网络保姆"所查

封。维护真理、公义和网络空间的人们只要进到这些软件过滤出的有碍字眼库里看一看，就会发现所谓的可疑条目辑录得实在令人莫名其妙。冒犯这些审查官的人们的遭遇也很令人回味。比如电子杂志《伦理现象》[1]的主编约翰森·威勒斯的经历就很有意思。在他谴责“网络阿姨”行为不端之后，《伦理现象》杂志就被“网络阿姨”禁止登录了。同样的事情也发生在本内特·哈瑟尔顿身上。哈瑟尔顿还是学生，创设了“青少年反审查联盟和平之火”[2]网。该网站是通过“媒体3技术”服务商进入因特网的。麦尔伯恩于是找到“媒体3技术”服务商，要求他们清除“捣乱分子”，遭到后者的拒绝。麦尔伯恩当即还以颜色：他不仅封闭了和平之火网站，而且禁止登录“媒体3技术”所运载的所有网站。格伦·罗伯茨的遭遇也大同小异：他的站点和域名 ripco.com 都被禁止登录。显然，道德律令和言论自由同床异梦，同室操戈。

经1995年7月14日投票表决、并于1996年2月获得批准后的埃克森修正案有所修改，用硅谷一家日报的话说，“改得荒唐程度低了一点”。修正案仍然要求服务商密切监督流经他们网络的所有电子邮件和内容。法案规定，任何服务商，不论通过电话或电子通讯装置，向

---

① www.spectacle.org/

② http://peacefire.org/

任何18岁以下未成年人士，或未经同意而向其他任何人制作、传输、或以其它有效方式生成（直接或通过复录装置）任何以商业为目的的不正当通讯，不论此类通讯的制作者是否拨打号码，或主动发起通讯"，皆可以受到起诉，并被判处最高达10万美元的罚款和两年监禁。

于是，在1995年夏，一向自成一体、不受限制、不可控制、也常常不负责任的网络自由，遭受了沉重的打击。许多团体为此奔走呼号，力图证明《正当通讯法》是非法的法律，违背了第一修正案的言论自由权。国会表决后数周之内，因特网民权联盟（Citizens Internet Empowerment Coalition）就向费城联邦法院提起诉讼。这个组织同美国民权自由联盟挂钩，成员包括因特网服务商、图书馆、出版社、报社、娱乐公司，还有5.5万名个人成员。该案后来成为美国大学法学院的研究案例，被称作"美国民权自由联盟对雷诺案"，因克林顿的司法部长名叫珍妮特·雷诺。

最高法院首席法官多洛雷斯·K·斯洛威特、最高法院法官斯图沃特·达尔泽尔和罗纳德·J·巴克沃尔特斯最早对这一案例进行了研究。他们恐怕没想到，他们之后不久作出的决定将使网络空间一片欢腾。1996年6月11日，三位法官判定《正当通讯法》违宪，其法理逻辑基于两个集中的推论：第一，他们根据电子边疆基金会律师的解释，断言任何思想传播都"必须或多或少地

作为传统媒体来对待，因而应该得到最高层次的宪法保护，这在宪法律师速记簿里，被称为‘严格审核’。第二点理由则是根据前最高法院法官罗伯特·杰克逊在1949年作出的一项裁决：“银幕、广播、报纸、传单、广播车和街头演说家，本质不同，价值各异，各有其弊端和危险。各自均可……独行其是。”

法官达尔泽尔明确解释了他在判决此案时赞同原告的理由：“可以毫不夸大地得出结论说，因特网已经成为，并将继续成为我国——事实上是整个世界——前所未睹的最大多数人参与的大众言论场所。案中原告正确地描述了因特网通讯的‘民主化’效应：即手段有限的个体公民能够向全世界听众谈论他们共同关心的问题。”费城法官们毫不含糊地说：不仅因特网应该依旧不受限制，而且还应该由父母，而不是政府来确定因特网内容的儿童不宜尺度。法官们发现《正当通讯法》企图钳制因特网言论自由，这是不可接受和不能允许的。达尔泽尔说：“实际上，政府之所以断言因特网‘失败’，乃是基于这么一个潜在前提，即因特网媒体上的言论太多了，这些言论对上网者来说太唾手可得了。但是，这恰恰是因特网通讯的好处。因此，政府是在含蓄地要求本法庭限制因特网上言论的总量及其传播。政府的论辩与第一修正案的原则存在深刻的分歧。”

三个星期后的1996年7月29日，三位曼哈顿联邦法庭法官肯定了这一判决，宣布《正当通讯法》违宪。

虽然如此，但过滤软件仍在使用，价格低廉，效果显著。而且，虽然裁决已下，克林顿总统仍无意改弦更张。正值1996年总统竞选全面展开之际，他不想为此冒犯保守的选民。费城联邦法庭作出判决不久，克林顿发表声明，表示坚持原有立场，继续支持《正当通讯法》。他在声明中说："一如当初签署这一法案之时，我仍然相信宪法允许我们通过实施这一法案，帮助父母避免儿童受到通过计算机网络传输的令人厌恶的内容的侵扰。我将在任内继续尽我所能向美国家庭提供所有有效工具来保护儿童远离这些东西。比如说，我们强烈支持开发和普及能让父母和学校禁止儿童用计算机登录令人厌恶的内容的产品。我们也支持计算机业加速努力，配合过滤技术，为因特网站点分等定级。"

1996年12月6日，最高法院决定审理联邦政府就费城判决提起的上诉。1997年1月21日，政府在一份司法部摘要中声称："父母及其子女享有第一修正案规定的接受信息和获得知识的权利，而因特网增进这一权益的潜力是无与伦比的。倘若人们因不愿子女受到明显令人厌恶的色情内容伤害的缘故，拒绝享受因特网的这些好处，那么作为教育和信息资源，因特网的大量潜力将被白白浪费了。因此，政府不仅在保护儿童远离网上明显令人厌恶的内容方面有格外强烈的利害关系，在增进所有美国人使用因特网这一无可比拟的教育资源，从而更好地享受第一修正案的权益方面，也有同样迫切的

利害关系。1996 年的《正当通讯法》增进这些利益的做法是合乎宪法规定的。”同一天，多家保守组织联合发表声明，支持政府的举措。声明说：“因特网上的色情内容对儿童构成独特的危险，要求国会作出新的回应。制订关于这一崭新的通讯媒介的法律成为当务之急。在法院先前的决定中，业已肯定了国会顺应（第一修正案）言论自由条款制订有关法律的权力。因特网从无数信息源中收集信息的能力使儿童不必迈出家门，就能够看到无限多的色情内容。”1997 年 3 月 19 日，双方律师对簿公堂。

1997 年 6 月 26 日，美国最高法院以七票对两票，确认第一修正案的原则，最终敲响《正当通讯法》的丧钟。最高法院宣称，因特网言论必须和报纸言论一样自由。最高法院法官约翰·保罗·斯蒂芬斯表述了多数法官的看法：“遵循宪法传统，在缺少相反证据的情况下，我们假定政府管制言论内容不管在什么程度上都与其说是鼓励，更不如说是妨碍了思想的自由交流。在一个民主社会，鼓励自由表达的利益大于新闻审查所带来的任何未经证实的理论上的好处。”最后裁决发布不到半个小时，就在网上流传开来。批准《正当通讯法》成为法律的克林顿总统反应如下：“对因特网，我们能够而且必须找出这样一种解决办法：它之于计算机要像 V 芯片之于电视一样有效，并且是以符合美国言论自由价值观的方式来保护儿童。依赖正确的技术和分等定级系

统，将有助于我们确保孩子们不会最后迷失在网络空间的红灯区中。”

不管怎样，还不到一个星期，比尔·克林顿就于7月1日利用最高法院的决定采取措施，为因特网走向成熟铺路架桥。时逢艾拉·马加齐纳发布《全球电子商务架构》报告，强调允许私营部门自由发展因特网的必要性。克林顿在报告发布会上声称：“因特网具有爆炸性的繁荣潜力，它应当成为全球性自由贸易区。政府应当对因特网竭尽全力，首先是不挡道，不妨害。我们要鼓励私营部门尽可能自己管理自己，我们要鼓励所有国家不征收歧视性税种和关税，或者加诸累赘的官僚主义……如果说有什么领域需要政府干预，那就应该是扶持一个可预见的、持续的合法交易环境。”

显然，在这两份声明中，最高法院和总统采取了符合因特网传统及得到恰当理解的因特网用户自身利益的做法，从而重振美国对网络的主导地位。美国因特网开发商充满活力、财雄势厚、现在又摆脱了内部法律的羁绊。他们有本事在全世界贯彻这些自由原则。有什么能够阻挡他们呢？

第三章 加密，自由之岛

不忆何年何月何时起，人类就殚精竭虑要保守通讯秘密。不同的文明为此创造了大量的加密系统，它们的军队、政府和特工籍此防范信息外泄。其中以德国的“谜语机”成就最高。这个加密系统达到巴别塔式的完美，1919 年获得专利后立即被德皇家谍报机构投入使用。

谜语机发明 20 年之后，第二次世界大战即将爆发之前，盟国开始通过人事渠道，零零碎碎地弄到一些有关谜语机的有趣资料——法国反谍报特工移交了一位纳粹高级官员，后者最早提供了谜语机的部分情况。谜语机是围绕三个旋转器建造的，到 1938 年后改为五个旋转器，可让字母表中的一个字母转变成另一个字母。但是，能干的德国技术人员后来把谜语机搞得高度错综复杂，以致于战前能破解其密码的波兰数学家不再能依赖

法国谍报机构的这些情报从事破译工作[1]。

从谜语机到PGP加密程序

不过，拆分这些融为一体的密码，发现背后的运作规则，需要一群杰出数学家的劳动。在伦敦附近的布莱奇利公园，阿兰·图灵领导的政府代码和密码学院终于学会译读谜语机的信息，解码就像看本打开的书一样容易。从二战爆发时起，图灵就致力于加密术研究，制造了一台可以自动进行所有可能破解谜语机的字句组合的机器。有件事说起来对充分认识他们工作的价值很有帮助——计算器正是为了破解谜语机才发明出来的，阿兰·图灵也正是因此赢得了“现代计算机之父”的称誉[2]。1946年，J·普罗斯珀·埃克特和约翰·W·毛赫利领导的小组在阿伯丁大学安装了电子数字整合分析器（E-NIAC），图灵没有参与此项工作。随着战争的结束，许多这类项目的资助停止了，围绕电子数字整合分析器的工作也暂告一段落。但杰出的匈牙利数学家约翰·冯·纽曼——他曾参与制造第一颗原子弹——继续在这一领域

① 谜语机历史参看：http：//members.gnn.com/nbrass/biblio.html

② 实际上，关于第一台计算机的真正发明者仍有某些争议。有些人认为真正的计算机必须可以编程，这是早期计算器所不具备的。维护图灵计算机之父称号的人则断言，图灵在1936年就想到了编程，并在他的大学论文里阐述了编程原则。

取得理论上的进展，并受图灵观点的启发，制造出一台新机器。他把他在 1944 年制造的这种机器称作“电子分离式可调计算机”（EDVAC）。图灵在战后也没有松劲，于 1948 年在英格兰曼彻斯特和迈克斯·纽曼小组一道研制出 Mark 1。Mark 1 可以说是真正意义上的第一台计算机，它有较大的内存，能够执行一个预设程序，而且使用了一台内部中央处理器。

无可争议，计算机科学的呱呱坠地，很大程度上要归功于科学家们为制造和破解谜语机所做的百般努力。实际上，科学家们围绕谜语机所做的工作极其浩大，这一过程中产生的许多发明创造半个多世纪以来一直被列入严格保密范畴，不为常人所知。传说二战期间，英国解码员得知纳粹德国计划轰炸英国城市考文垂，却没有对考文垂居民发出任何警告，只因为担心德国人因此知道谜语机已被破译。英国矢口否认了这些说法（在 1940 年 8 月 17 日和 11 月 14 日至 15 日，及 1941 年 4 月 8 日和 10 日，纳粹德国轰炸考文垂，致使 1200 人丧生，6.8 万座建筑物被毁）。其实，1940 年 6 月至 12 月间，图灵和他的同事们使用的模拟谜语机所产生的信息中，仅仅只有五道被破译。1941 年 5 月 19 日德战舰“俾斯麦”号离开基尔港时，他们花了三天时间才破译出指挥官的电报。直到 1941 年夏天，图灵及其同事才开始非常有规律地破译谜语机信息。

战后，计算机科学的诞生导致密码技术突飞猛进，

一日千里。科学家们一方面制造出越来越“复杂”的密匙来保证信息安全，另一方面又运用计算机手段克服了解码过程中日益难以逾越的障碍。基本上，科学家们是经过反复试验、不断摸索后，搞清楚被使用的密匙的类型，然后再尝试所有想得到的组合。其实，这些手段和小孩用一个字母代替另一个字母的方式加密并没有多大差别。任何人只要知道密匙，阅读加密文件就和小孩子作游戏一样：直接将合适的字母替代进去就可以读到原来的文本。因此，这样一个系统最薄弱的环节之一就是加密者需要将加密办法送给解密者。

世界各国的谍报机构都在为破解使馆和其本国政府秘密通讯的代码而耗费时间和金钱，这也是美国国家安全局的主要工作之一。国家安全局的预算要比中央情报局多得多，它把最能干的美国数学家几乎全部招致麾下，其中大多数人一生都在为政府工作。计算机科学，就像它刚刚诞生时那样，依然和需要进行大量运算的破译密码工作息息相关。法国也深深投入了解码工作，法国国外安全总局巴黎总部的整个地下室里都装满了克雷计算机，其中有些计算机是世界上威力最强大的。和其美国同行一样，法国国外安全总局也招募了法国第一流的数学家，让他们在雷恩附近的布吕兹电子武器中心的中央办公室工作。

所有这些专家都精通多维空间的技巧。他们创造的代码系统被称为密码（ciphers），这也是对所有各种代

码和数字的通称。加密术就是创造和使用这些密码的学问；而从事代码破译和数字捣弄的人就是密码分析家。加密术就是密码和密码分析的结合。无论使用代码或密码，把一个正常文本变成用代码或密码写成的文本，就是加密[①]。时至今日，代码不再只是一个字母代替另一个字母的简单把戏，也不再像约翰·勒·卡雷的优秀作品《完美的间谍》中描述的那样，用两本同样的书，在书中的字词下面划道道。

共用密匙……个人密匙

现代加密系统使用的是一系列非常复杂的加密运算法则。而且，尽管必须用威力强大的计算机来揭开代码后隐藏的秘密，耐心、运气和不屈不挠的精神往往是解密武器库中最有价值的工具。

美国最常见的加密系统之一是数据加密标准（DES），它在金融交易中应用尤其广泛。数据加密标准最早是在1976年由国家标准和技术研究所（当时称为国家标准局）授权使用的。它获得通过后，被用于商业和满足"敏感但未列入机密级"的政府需要，但不用于

① 如果读者想对加密术有更多了解，可在以下新闻组里找到一个非常出色的每隔21天张贴的加密答疑（FAQ）：sci.crypt、talk.politics.crypto、sci.answers和news.answers.

真正机密的工作。数据加密标准系统是由美国国际商用机器公司在国家安全局协作下发明的，起初被称作“魔鬼”（Lucifer）。这个加密系统的保密能力已经降级，现在它使用的系列密匙由 56 比特组成，每把密匙又由 87 比特的字节或计算机字符组成。

数据加密标准灵活实用，多年来演变出许多不同的版本。尽管按照摩尔定律（每 18 个月计算能力增加一倍），数据加密标准的安全性和能力随着时间流逝在削弱，但它看起来仍有多层次的用途。它的最新版本是三重数据加密标准，其中两到三套密匙被混合在一起使用，破解一道加密信息需要大量命令，从而使解码更加困难。不过，得警告一下业余加密术研究者：在美国和在世界其它地方一样，政府认可某个特殊的加密系统，这事实上等于宣布该政府自有破译之道。

最好的密码当然是谍报机构留给自己用的密码，而且永远不会在市场上出现。就我们所知，所有间谍及其雇主之间的通讯系统，不论他们在何时何地出现，都掌握着某种密匙：文本 A 经使用密匙 C 转变成文本 B。不管谁有密匙都可以把文本 A 转换成文本 B，或者把文本 B 转换成文本 A。理想的解密方案是同时拥有文本 A 和文本 B，从中推演出密匙 C。这种加密系统的脆弱之处在于密匙必须以某种方式送达接收加密信息的人或组织。

1975 年 5 月，斯坦福大学两位学者——怀特费尔德

·迪非和马丁·海尔曼，发明了一种为信息译码的新方法，从而给老式加密方法奏响了最后的挽歌。迪非当时只有 31 岁，是加密领域不折不扣的怪才。他从小就对数学着迷，成年后曾在太阳微电子公司工作，在那里备受推崇。他和海尔曼创立的加密系统不需要交换密匙。

假设杰克打算和姬儿密谈。首先，杰克弄了两把密匙，一把是个人的，一把是共用的。杰克自己留着个人密匙，把共用密匙放在网上某个地方。现在姬儿有秘密消息要发给杰克，她在一家人人都能进入的在线电子图书馆里找到杰克的共用密匙，用它给文件加密，杰克的密匙就把姬儿的话全变成了胡言乱语。然后姬儿把文件传给了杰克，任何截取文件的人都会发现这个全是代码的文件没有任何加密的密匙，甚至姬儿自己也不能读懂，但杰克却可以。当他收到文件，他取出自己的个人密匙就能够打开文件。反过来，如果杰克想要给姬儿写信，他只需找到姬儿的共用密匙来给自己的文件加密，也只有姬儿本人用她的个人密匙才能打开并看到这个文件，而姬儿的个人密匙可以保存在磁盘里、家里、保险箱里或别的什么地方。这一来，再也不用为处理密匙发愁了，每个人都有自己的密匙，就在自己的身边。

回过头来看，当因特网如初生婴儿般第一次蹒跚迈步的时候，这一共用密匙系统蕴藏的原理就已宣告了因特网日后大踏步的跃进。当时，只有政府机构在使用代码，也仅仅只是使用。现在，加密术在各行各业用户中

流行开来。实际上，共用密匙的观念和应用带来史无前例的进步。使用共用密匙不仅传递加密信息时不用担心网络警察或好事的黑客窃听，而且还能证明信息的真实性，确保发送者就是声称发送信息的那个人。

1977年，三位麻省理工学院学者（荣·瑞沃斯特、艾迪·沙米尔和列奥纳德·艾德尔曼）研制出RSA加密程序（RSA是三人姓氏的首字母——译者）。这是最早堪与数据加密标准争雄的共用密匙系统之一。没过多久，最著名的编码器就把RSA和数据加密标准合在一起用，以此成倍地增加自身的安全性。比如说，杰克首先用一把数据加密标准密匙给自己的信息加密，然后再用姬儿的共用密匙给数据加密标准密匙加密。姬儿收到杰克的信息后，先打开数据加密标准密匙，再用她的个人密匙给信息解密。

虽然RSA之后还有其它共用密匙系统被开发出来，但RSA已成为美国最尖端的政府系统使用的某种规范。引人注目的是，不仅美国核武器发射密码赖RSA以保障其安全，俄罗斯核武器发射密码也是用RSA来保护的[①]！

---

① 据美联社1999年8月27日电，荷兰阿姆斯特丹国立数学和计算机科学研究所的研究人员当天说，他们花了6个星期时间，使用一台克雷900-16超级计算机，300台个人计算机以及专门设计的软件，破译了RSA-155密码。——译者

为何还烦恼?

如果从来不曾有人想到，有朝一日，普通百姓能够自己给电话改频以防窃听，那只是因为还不存在能达到这一目的的比较基本的手段；又或者是因为当局依靠严刑峻法的震慑，把这些手段的使用范围限制在高级官员、警察或军队之中。但到1995年年初，“鹦鹉螺”尖端武器研制项目启动之际，情况发生了变化：计算机变成无法窃听的电话。

电话是一种令人放心的耐用的通讯手段，其基本技术只能提供声音传输（有时效果不很好），但应用遍及全球，其优势有目共睹。不管怎样，人们现在不再满足于只能听到声音。在因特网时代，一台普通微机和一个便宜的调制解调器就可以更加有效地利用那些老旧的铜电话线，向全球发送数以十亿字节计的各种信息和电子邮件，费用不过是本地电话费而已。

但是，难就难在这里了：通讯数字化好比天赐给搞窃听工作的“老大哥”[1]们的礼物。不论他们是从电话

---

① “老大哥”一词出自英国作家乔治·奥威尔著名的反乌托邦政治讽刺小说《一九八四》，指无处不在的窃听和监视公民个人生活的独裁者。这本书风靡多年，已成经典，作者的名字因此也演变成形容词，所谓“奥威尔式”云云，盖指受严酷统治而失去人性的社会的……，后文出现过多处。——译者

线还是卫星传输，或者从因特网节点截取信息，这些信息的电子本质意味着：一辆没有标志的货车停在黑暗的小巷，车上满载监听设备和受过高级训练的窃听者，这种事已成历史。窃听者不必再侧耳倾听，他们可以单纯地从传输线上攫取信息比特，然后从中过滤出加过密的精华部分。从本质上说，探听他人隐私这一行当内部发生了瓦特发明蒸汽机式的工业革命。不论是事实还是出于想象，没有人能再保证不被另外某某人窃听。尽管谍报机构针对公民个人自由的行动受到各种规定约束，但各种窃听方式是如此易行，以致现在政府谍报机构和私人机构都可能会越来越频繁地进行窃听，而不是相反。所有的国际通讯都受到监督——尽管是随机性的，但总归是监督。在窃听领域，蒙昧的极权主义政体和民主化程度很高的国家可谓平分秋色，都能当上世界冠军。

显而易见，世界警察打着捍卫民主的旗号，过去在不舍昼夜地侵犯平民的个人自由，现在也仍然在逐渐而巧妙地渗透进信息网络，就像从前窃听电话一样。一旦遭到质问，他们的辩解全都如出一辙：他们只是在运用其职权所允许的手段打击毒品交易、大宗盗窃以及各式各样的间谍活动。他们断言，为了抓住这些坏蛋，需要合法地探明大多数人的隐私。法律保护个人生活隐私，其中一条基本原则就是家庭不可侵犯；法律也保证政府司法部门有权进行搜查，但是只有在证据确凿、法庭认定有此需要之后，并且是在被监视者获得某种不管多么

基本的法律帮助之后才能进行搜查。如果这的确适用于一般通讯方式，那么，网络空间也应该享有同样的待遇。

你喜欢也好，不喜欢也罢，假若你不想让网上通讯遭到窃听，那只有一个现实的解决办法：加密。这是阻止谍报人员、网络管理员和形形色色的黑客潜入我们个人生活的唯一办法。当然，有的编码系统比别的更出色。使用加密技术和使用别的任何东西一样，你得为之付出代价。另外，我们中的大多数人可能想花上一笔钱，就在书房架子上，挨着索尼音响和录像机摆一台属于自己的小型谜语机，这是不太可能的。

但是，随着 PGP 加密系统的推出，一切可能都将为之改观。PGP 有百分之五十的把握能使密码不可被破解，这使得谍报机构现在坐立不安，苦谋重组。谍报机构之惊惶程度反映出 PGP 革命的影响之大。一道屏障，一堵保护大众隐私的围墙矗立起来了。

世上有了 PGP

PGP 的威力在于它成功地把另外三个加密系统——RSA、IDEA 和 MD5——融为一体。虽然 PGP 的发明者菲尔·兹默曼十分谦虚，总爱说他的软件提供的隐私保护“还不错”（Pretty Good Privacy，PGP 即这三个单词的首字母缩写），但这个程序几个月内就风靡世界，令奥

威尔式的窃听者们大为气恼。

不过，要不是有 IDEA 出现在先，PGP 还不会这样出风头。IDEA，全称是国际数据加密算法系统，1990年由詹姆斯·L·马塞和赖学嘉（音译）在瑞士苏黎世推出。PGP 正是借鉴了 IDEA 的创新性加密方法，使得现在用 PGP 加密的文本——甚至是用完全相同的密码加密的完全相同的文本——第二次的面目也永远不会和第一次一样。IDEA 是把文本作为一个整体来译码，所用密匙长 128 比特。对所有民间研究者来说，破译 IDEA 已经成了上瘾的游戏。但不管是他们，还是他们在谍报机构的同行（尽管他们就算破译了也不会公开吹嘘一番），谁都没能拿下 IDEA。

假设（从理论上）一台微机的运算速度极快，能够每秒验证一百万个不同的密匙。现在再设想有十亿台这样的计算机同时在这样做，要把 128 比特全部可能的排列组合都试一遍也需要一百亿年。计算机的速度一直在提高，成本也在迅速下降，但对 IDEA 这种无理性的破译方式仍恐怕永远都不会成功。唯一有可能成功的破译模式就是尝试分析纯文本单元之间发生的转换及其对等的密码内容，从数学角度解决这个问题。IDEA 还有一套相当新颖的计算法则，牵扯的理论较复杂，攻克 IDEA 也得在这方面下功夫。不过迄今为止，似乎还没有比无理性攻击更合适的破译 IDEA 密码的计算法则，而这么做我们早已说明是不可能的了。IDEA 内部的非

线性转换使它成为极其难以解决的数学问题之一[1]。

除 IDEA 之外，PGP 的最新版本（MIT 2.6.2，Viacrypt 2.7.1）还继续使用了 RSA 的“不对称加密”的概念。这样就可以管理长达 1,024 比特的密匙（308 位数字，实际上是 2,048 比特）。直接成功破解这样一把密匙的可能性是不存在的。如果说，成功地直接破解一把长度为 128 比特的密匙需要 100 亿年，那么破解 2,048 比特长的密匙所需时间就是 100 亿年的 5 次方，这是一个长达 259 位的天文数字。当然，加密专家明白你不会硬碰硬地攻击不对称系统[2]。最好的办法——数学家所欣赏的办法——是将一个和密匙等长的数字分解因子。1994 年，有 1,600 名学者经过一年多时间的工作，通过因特网链接了世界各地成千上万的微机，才成功地将一个 129 位的数字分解因子。值得一提的是，任何使用长度超过 128 比特的密匙的人都有点走极端。在信赖 PGP 给文件加密的人当中，这种偏执狂还很常见。他们必须听到 PGP 系统推销者一般推荐使用由 512 比特（154 位数字）组成的密匙，才会感到最大程度的安心。

布鲁斯·施内尔曾经计算出，要达到这个数字需要

---

① 参考网址：http://www.praoroenet.org/jalicqui/pgpgaq.txt 或 alt.security.pgp

② 不对称加密法是共用密匙加密法的另一种称谓。因为这种加密法所依据的计算法则能够使给信息加密的共用密匙和给信息解密的个人密匙互不相同，但彼此存在某种数学上的联系。

花100万美元。估计到了2010年，以计算机科学为基础的信息成本将会大大降低，到那时这么做大概只要一万美元，但你还得花3千万亿美元来破解308位数的密匙。在某些圈子里，这种理论上的推演引起无穷无尽的争吵，使人们认识到，正如当代计算机技术脱胎于破解谜语机的需要一样，阻止RSA和PGP大行其道也将成为催生未来几代计算机的动力。

应当非常清楚的是，如果你能得到某人的个人密匙，破译密码就毫无难处。因此，谍报机构只消又干上诸如闯入民宅之类的拿手好戏，就能够把事情大大简单化。对使用PGP的人来说，保护个人口令则成了头号要务。菲尔·兹默曼仔细考虑了这个问题，简洁地强调了保护个人密匙所应当采取的措施。他说："为了保护密匙，你要从一开始就总是把它放在自己够得着的地方。可以把它存在家里的个人计算机里，也可以放在你能随身携带的笔记本计算机里。你必须只在你能实际控制的计算机上使用密匙，不要在存放密匙文件的计算机里的任何地方存放口令段。把密匙和口令存放在同一台计算机里就和把你的自动取款机银行卡及其密码放在一个钱包里一样危险。如果你只用脑子记住口令段，别的什么地方都不放，那就再安全不过了。要是你感到非得把口令段写下来不可，那就保管好，可能甚至得比保管密匙文件更小心……没有牢不可破的数据安全系统，人们能够用各种方式智取PGP。不论何种数据安全系统，

你都得问问自己，你试图保护的信息对你的对手来讲，是否价值超过破解它的费用，这应当使你能够免于遭受最廉价的解密攻击，同时也不用担心费用更昂贵的袭击。下述讨论有些看起来可能过分杞人忧天，但这样一种态度正适于理性地探讨脆弱性问题。”菲尔大叔的建议确乎是金玉良言。

收藏这些笨重的数字密匙，并记住它们冗长的字符串是不可能的，但办法还是有的，当然你不能把它用大号贴纸抄下来粘贴在计算机显示器上。有种办法是利用智能软盘来保存密匙。它的外观和一张标准的3.5英寸软盘并无二致，但里面装有微处理器和可与磁盘只读器磁头直接交换指令的界面。这张小小软盘可以随机产生共用密匙和私人密匙，但甚至用户本人也只知道共用密匙，而不知道私人密匙。软盘可以被复制，弄丢了绝对不是什么好事。

PGP 和因特网

菲尔·兹默曼早年十分激进，曾经为抗议核军备而两度坐牢。虽然现在成了计算机分析专家，他仍然是位好战的和平主义者。鉴于 RSA 共用密匙系统至今都过于复杂，实际上只能应用于大型、昂贵的计算机系统，兹默曼开始着手改进 RSA，力求使之适于个人计算机使用。兹默曼把他的专业能力，连同他的政治信仰和对加

密术的狂热爱好都揉合到这一工作之中。他在 1977 年就萌发了这个想法，但直到 1984 年，这项工作才成为他生活的重中之重，令他日以继夜地为之奋斗。那时兹默曼就如同着了魔一般，经常忘记付帐单，而且差点失去他在科罗拉多州博尔德的房子。直到 1991 年，兹默曼才最终制作出他满意的产品。他在几年后写道："PGP 也有着深远的政治内涵，其中绝大多数是积极的。在信息时代，加密技术影响了政府及其人民之间的权力关系。政府对此心知肚明，证据就是他们最近推出的解码器计划。解码器将给政府开个后门，使政府可以监听所有的私人通讯——在所有电话、传真机和计算机网络上装上奥威尔式的'窃听芯片'。PGP 对这股黑潮予以迎头痛击，从而成为加密术革命发展的晶核。而加密术革命乃是信息时代捍卫个人隐私和自由的一场新政治运动，政府业已竭尽所能来阻挠令它无隙可乘的全球性加密标准的出现。"政府机关算尽，但终归徒劳，因为 PGP 已经成为这样的全球性加密标准。

兹默曼拒绝出售他的程序。和所有优秀的计算机科学家一样，他渴望看到每个人都能用他的软件。一俟他完成并测试了 PGP 的第一个版本（当时还只能在 PC 格式下运行），他的一位朋友就立刻把它张贴在 BBS 上，任何人都可以通过因特网免费下载。1991 年 6 月的一天，几个小时之内，全美成千上万台计算机都下载了 PGP 程序。几天后，兹默曼开始收到来自世界各地的电

子邮件。

经过这么多年的苦心准备，兹默曼急于把 PGP 投入使用，这不是偶然的。他已听说参议院正在讨论一项试图限制普通百姓接触加密技术的法案，而且意识到 PGP 将使法案半途而废。

兹默曼狂热地致力于完善 PGP 程序，但在细节问题上没费太多心思，这中间就出了问题——PGP 程序借用了 RSA 的部分内容，但他却忽略了征求 RSA 合法所有者同意。兹默曼为此官司缠身，遭到巨额经济威胁，直到 1993 年 9 月始与 RSA 商业执照持有者 Viacrypt 公司达成了协议。

摆脱官司后，兹默曼转而从商。按《福布斯》杂志的说法，到 1996 年，兹默曼赚的钱就超过了 800 万美元。他因此不仅得以于 1996 年 1 月自创 PGP 公司，而且还在当年 7 月买下了 Viacrypt 公司。时任董事长和首席执行官（CEO）的兹默曼随后请来了诺韦尔（Novell）公司前总裁托马斯·斯坦汀博士担任 PGP 公司总裁和首席执行官。到 1997 年，PGP 公司已聘用了 40 位程序设计员，现在又在设立分公司，而且仍在准备扩大。你就想想有多少人打算花 149 美元购买 PGP 吧：视窗 3、DOS、麦金托什和尤尼克斯（UNIX，一种多用户的计算机操作系统）的用户使用 PGPmail，视窗 95/NT 的用户能用 PGPmail4.5 以及确保网络使用安全的 PGPcookie cutter。他们全都可以得到用于给电话通讯加密的 PGP-

phone 软件。PGP 还有免费版本（PGP 2.6.2 和 PGPphone1.0），可从与 PGP 公司 有合作关系的麻省理工学院网址 http：//web.mit.edu/network/pgp.html 上下载。不过，请注意，非美国公民被禁止从国际上获得 PGP 商业产品，或从麻省理工学院网址免费下载 PGP。

网络烈士圣兹默曼

经历所有这些商海沉浮，最终安然无恙的商人们，信心十足，心情迫切，急于把这种完美的秘密通讯手段推销给上网冲浪的人们。但是，菲尔·兹默曼不幸却卷入险恶的风波，他遇到的对手是比商海鲨鱼更难对付的美国政府。

在加密术领域，国家安全局曾包打天下，唯我独尊，共用密匙的发明改变了这一局面。而兹默曼的出场仿佛制造了一场出人意料的爆炸。几十年来，国家安全局在使用加密术时一直所向无敌，它把工作重点放在破译外交通讯所用的密码上，因而不想为国内密码操心。数据加密标准这类的美国加密系统早已在国家安全局视野之中——而且万一没有拿到密匙，它也能够拿根牙签硬捅进去（虽然国际商用机器公司发表声明否认这一点）。正如约翰·派里·巴劳 1992 年 7 月在《迷宫解密》一文中所言："国家安全局时刻监督着加密技术。它一贯推行的政策就是：如果有什么包含加密方法的设置或

者程序是国家安全局所难以破解的，它就要禁止这一技术在国际上销售。这项政策从未引起争议，甚至也不被承认。我对国家安全局竟然试图禁止某些算法系统感到十分惊讶：这种行径不仅愚蠢，而且就像限制出口风一样不切实际。此外我很少理会国家安全局的加密政策。”

国家安全局和大企业之间有过一些成功的合作范例。美国移动电话网使用的加密系统在谍报机构眼中就是“透明的”，其软件的各种“出口”版本的口令破解起来容易得令人吃惊。国家安全局甚至禁止国际商用机器公司在其 AS/390 机型中安装加密微处理器。

PGP 的诞生令国家安全局犹如碰着充满电的高压电线一般，大受震荡。国家安全局决意报复。但是，美国宪法既保护言论自由，也赋予美国人自行为通讯加密的权利。兹默曼不遵守国家安全局单方面制订的游戏规则这一事实改变不了这一点。不论 PGP 是不是一场革命，也不论国家安全局能否破解 PGP，兹默曼都受到宪法第一修正案的保护。国家安全局没法从这方面起诉他。

因此国家安全局就另外想办法对付兹默曼。兹默曼被告上了法庭——虽然他的案子是否和迷宫般的国家安全局有关始终得不到证实。在加利福尼亚州圣何塞，一位法官直接向兹默曼开火，判定能够按照《国际武器流通规定》以非法出口武器罪审判兹默曼。《国际武器流通规定》公开而且直接唯国家安全局的利益马首是瞻，它所准许出口的唯一的加密系统柔弱得就跟小猫一样，

密匙不超过40比特。如果PGP流传到国外，国家安全局就无法破译大量有关美国国家安全的情报。

这个理由十分有力，围绕它出现了激烈的争论。乔治敦大学一流加密专家多萝西·邓宁在《在线》杂志上发表的文章极大地唤起了激进派加密学者的普遍警惕。邓宁在文章中写道："如果我们不能立法以确保在法庭授权下持续进行电子监视的能力，如果法律没有对经法庭授权的窃听作出适当规定，社会就将成为犯罪分子逍遥自在的'动物保护区'，里面犯罪集团头目、毒品贩子、恐怖主义者，以及其他罪犯可以为所欲为而不受惩罚。最终，我们将发现反社会的严重犯罪在增多，打击严重犯罪的能力却大大萎缩，而且没有及时的解决办法。"计算机科学信息专家多恩·帕克补充说："我们拥有百分之百的保护隐私能力。但如果大家都利用这份能力，我认为社会就将无法维系下去。"对此，巴劳则模仿国家安全局的口吻嘲讽地回答道："你可以得到我的加密运算法则……当我握着个人密匙的手指变得冰冷僵硬时，你把我的手指使劲掰开就行了。"

日趋激烈的争论中产生出一批新的激进派，这就是计算机朋客（cyberpunk）。计算机朋客擅长编写确保私人通讯不被侵犯的加密程序。他们的宪章说："计算机朋客假定隐私是件好事，而且希望会有更多隐私不受侵犯。计算机朋客认识到，想保有私生活的人必须自己去努力，不能寄望于政府、大企业或其它大型的不露面的

组织出于仁慈之心来保障他们的隐私。计算机朋客知道，多少世纪以来，人们一直在借助于窃窃私语、信函往来、关门密谈和专人送信来保障个人隐私。计算机朋客不会设法阻止他人谈论有关经验或发表他们的观点……”

兹默曼想要改进 PGP，写出可对电话交谈加密的版本。不过，他感到他所研制出的加密工具，不管是优是劣，是好是坏，现在都属于整个社会。他说：“我不愿看到犯罪分子使用这项技术。假如我发明的是辆汽车，别人告诉我犯罪分子开着车抢了银行，我也会心情恶劣。但绝大多数人都不会对汽车带给这个社会的益处持有异议——汽车载着孩子们上学、购物等等，其利远大于其弊。”加密无政府主义者则把这一论点推向极限。

加密无政府主义者迈的步子更大。他们无惧于打着自由不可羁束的旗号进行挑衅，彼此交易制造炸弹的配方，还常常直接挑起与联邦政府的冲突。从网上可以看到梯莫西·梅撰写的《加密无政府主义者宣言》。梅曾为英特尔公司工作，30 岁时就拿到一笔颇为可观的股票买卖权退休。他毫不含糊地在宣言中亮出自己的意图，鼓吹把加密术作为获得完整的自由的一种手段：“……国家当然要援引国家安全考虑、毒品贩子和逃税者对加密技术的利用以及担心社会分崩离析等理由，试图放慢或阻止加密技术的传播。其中许多忧虑是有根据的：加密无政府主义将使得国家机密被任意买卖，非法和偷盗

得来的资料也可以被交易。一个匿名的计算机化市场甚至有可能造就出可恶的谋杀和敲诈市场。形形色色的犯罪分子和外来客都将成为加密网（CryptoNet）的热心用户。但是这都不能阻止加密无政府主义的传播。就和印刷术改变和削弱了中世纪帮会的权力以及社会权力结构一样，加密逻辑方法也将从根本上改变大公司和政府干预经济交易的本质。加密无政府主义将和新兴的信息市场一道，缔造出让所有能变成文字和图像的资料都可以在其中流动的市场。而且，就像带刺铁丝网这样一个看起来微不足道的发明使大面积的牧场和农场可以不必再安篱笆，从而永远改变了西部边疆土地和财产权观念一样，来自一个神秘的数学分支的貌似细小的发现也将成为剪断环绕知识产权的带刺铁丝网的带电剪刀。起来吧，除却带刺铁丝网的樊篱，你什么都不会失去！[①]”

这一激烈主张产生了某些不良的副作用。它允许美国右翼好战分子保持秘密联络，炸弹制造法以及种族主义理论轻易流传，而其它一些忘乎所以、极端主义的渣滓也趁机泛起。不论这些加密无政府主义者在网上说或写些什么，他们和企图消灭美国政府或联合国（有人视之为世界政府的雏形）的极端主义杀人狂没有分别，笔底全都蘸着赤裸裸、苦涩涩的反犹调味汁。

---

① 在网址：http：//swissnet.ai.mit.edu/6095/assorted - short - pieces/may - crypto - manifesto.html 中可以看到这份加密无政府主义者宣言。

看来，兹默曼势将成为美国政府的眼中钉、肉中刺；网络自由事业的烈士；追求更多隐私的象征。而作为这么一个象征，他本人也势将首当其冲地受到严厉的法律处置。但到1996年1月8日，兹默曼的律师菲尔·杜博伊斯万分惊奇地收到加利福尼亚北区助理检查官威廉·凯尼发来的一份传真，通知他说：兹默曼“将不会因1991年6月在USENET上张贴PGP加密程序被起诉，调查就此结束。”同一天的新闻公报上说：“对拒绝起诉的原因无可奉告。”加利福尼亚州检察官是在和司法部磋商之后作出这一决定的。这消息就像野火一样传遍了网络空间，世界各地成千上万的PGP用户为之喝彩，散布网络的PGP用户甚至创立了辩护基金来替兹默曼付律师费，他们的精诚团结显然得到了报偿。电子边疆基金会律师马克·葛德温在这场风波中自始至终支持兹默曼，他在司法部决定公布后说：“这真是政府的耻辱。他们想杀鸡儆猴，冻结加密技术在网上的传播，结果惹火反烧自家身。他们的所作所为使得许多人反对政府政策。”

站在兹默曼一边的不仅仅是网络空间的人权卫士——他们相信人人有权为通讯加密是保护个人私生活不受侵犯的最佳方式，许多公司也加入了抗议审判兹默曼的队伍。美国工商业人士享有在美国国内使用PGP软件的合法权利，但他们每次携带装有这个程序的膝上电脑出国时，就会冒违反《国际武器流通规定》法规的风

险，从而把自己置于不尴不尬的地位。而且，没人能否认像他们这种身份的人，需要和国内公司保持既隐秘又安全的联络。所以，既然工商业界理解和承认加密是绝对必要和需要的，美国政府就发觉自己是在和企业家作对。如果说违反美国法律暂时出口加密软件是场瘟疫，那么携带谁想偷看就能一览无余的计算机、程序和文件周游世界就是霍乱，美国企业家们可根本不打算被迫做这样的选择。由于美国政府准许出口的密匙只有 40 比特，出名的不堪一击，以致 1995 年 8 月 16 日，用来保护一流的因特网浏览器网景的密匙被一位法国青年破译。事情缘起于 1995 年 7 月，计算机朋客向一群加密专家提出了破译网景密匙的挑战。在一个周末，27 岁的达米安·多利盖兹只花了几个小时就首先大功告成。他使用了在隶属于法国国家计算机和电子研究所（INRIA）的 Rocquencourt 研究中心联网的 112 台个人计算机。另一攻关小组成员散居世界各地（包括英国的亚当·布莱克、瑞典的大卫·拜耶斯和澳大利亚的埃里克·扬），他们通过因特网合作，也获得了成功，与多利盖茨仅相差两个小时。所以，既然一位拥有优良硬件、水平出色的计算机科学家能够做到，又有什么是自视甚高的黑客做不到的呢？达米安·多利盖兹事后发表声明指出其中的风险：“某某人使用信用卡进行网上购物时，其号码就有可能被盗贼攫取以牟私利。”

追根溯源，许多加密系统之所以脆弱，部分原因得

归咎于数学家们为享受科学乐趣而破译它们的强烈嗜好。1996年4月10日，贝尔科尔的阿尔金·K·林斯特拉领导的研究小组宣布他们成功地分解了RSA—130的代码[①]，进一步强化了人们对需要用更长的密匙保护通讯秘密的想法。PGP使用的密匙就非常之长，从而免遭被破译的厄运。从这些事件中，可以得出结论：如果美国政府心甘情愿地允许广泛使用40比特的密匙，他们必定可以毫不为难地破解它；如果美国政府提议把限制放宽到56比特——1996年10月，美国政府宣布了这一举措——那么答案也还是一样。正是基于这一点，1996年6月26日，一群高级科学家借马修·布雷兹博士在美国参议院商业委员会科学、技术和空间附属委员会上发表演说之机，发表文章指出："值得庆幸的是，非常强大的加密系统，其费用并不比脆弱的系统高出很多。因此，要适当地防范最严重的威胁——树大根深的商企或政府情报部门——用以保护数据的密匙长度目前应该至少长75比特。在未来20年里，鉴于计算机能力意料之中的增长，新配置系统的密匙应该至少长达90比特才足以保护信息。"

PGP象征着政府挑起的旨在反对人人有权给通讯加密的斗争，其中有个很大的悖论，就是当局对必须依靠

---

① 想对此了解更多的读者，可访问：http：//www.napc.syr.edu/factoring/status.html

政府控制和渐进立法不可或缺这两点都认识得再清楚不过，否则，他们早就断绝了监视网络的任何念想，而那可绝对不在他们计划之中。随着欧洲开始在加密术领域东山再起，美国自从放弃解码器之后，也一直力图进行法制建设，谋求仰仗法律来限制所有个人用户和所有企业进行加密。这一切努力都基于这么一个不变的主导思想，那就是要以这样或那样的方式，让所有使用加密软件的用户都把密匙交给被授权的持有者，而警察和情报机构可以从后者那里得到这些密匙。1995 年 8 月 17 日，美国国家标准和技术研究所副主任雷·卡默在软件出版商协会召开的学术讨论会上透露，政府不久就将允许出口和美国本土所用的同样强大的加密程序，条件仍旧十分严格，因为“加密产品（必须）仍然为出口者或与之偕行的任何其他美国公民或合法永久居民所掌管，为其专用，不得用以复制、展示、营销、出售，所有权或控制权不得再出口或转让。”这是朝着正确方向迈出的一步，但还没有公然违背谍报机构的需要。1995 年 9 月 21 日，联邦调查局局长路易斯·弗里在国际加密研究所毫不含糊地表明自己的立场：“为了千方百计地维持公共安全——以及商业和国防安全——我们必须强力支持加密。但是，我们认为，经法庭授权获得解密方法，这一点需要维持原状。逾四分之一个世纪以来，不管违法者是恐怖分子、犯罪团伙、核走私犯、毒品贩子还是间谍，我们一直都以这种方式获得他们的谈话、记录和计

划。”

出路何在？1996年上半年，美国继续调整立场，国家研究委员会就此发表了一份厚厚的引人注目的研究报告，建议不必立法禁止出口加密系统，因为它们早已在世界各地广为使用。这场加密之争在美国几乎是公开的，有趣的是，它附带着对欧洲也产生了影响。法国过去在加密领域居于领先地位，它和其它许多欧洲国家一道，开始采取和美国十分相近的政策。1996年5月20日，加密政策部门间工作小组并列主席布鲁斯·W·麦克康内尔和爱德华·J·艾帕公开发表了白宫就此委托他们撰写的报告。报告本着赖以赢得抵制解码器胜利的原则，建议成立一个共用密匙和个人密匙管理组织机制，命名为密匙管理基本设施（KMI）。每个用户都要送交一套共用密匙和个人密匙，由一持有许可证的权威机构加以担保。第三方保管机构负责保存密匙，只有在密匙所有人受到调查和司法部发布许可令之后才能把密匙交给警察。一个月后，司法部长珍妮特·雷诺谈到这个问题，但没有澄清密匙管理基本设施如何运作以及由谁管理。对雷诺来说，实质问题就一个：“不可破译的加密系统的传播，事实上将产生更加广泛的影响，因为我们还将失去搜捕和查获被储存数据和其他形式的电子证据的能力。我们能够得到常规搜查令，但如果搜到的数据被加了密，除非拥有密匙，这个搜查令就是一张废纸。”雷诺态度鲜明，毫不含糊，对此，网民的反应和抵制解

码器时一样：隐私就是隐私，不管属于个人还是商业用户，没有人愿意放弃它。还在 1996 年夏季，论战双方压力与日俱增，这时华盛顿电子保密信息中心主席暨乔治敦大学法律中心教员马克·罗腾伯格在参议院发表演讲，义愤填膺地指责政府企图通过第三方保管密匙让解码器死灰复燃。他说："用户不仅仅只是反对政府掌握密匙的提议，他们反对的是旨在加强政府对私人通讯监视的技术。"电子保密信息中心和网上其他隐私卫士的观点是一样的，按它的说法，美国政府在乎的是谍报机构今后也能继续保有自由监听电子通讯的手段，就像现在监听电话通讯一样。罗腾伯格继续说："关键是要明白，白宫依然相信加密手段只应该在易于破解的条件下才可以被使用。政府的几项提议都以此为前提条件，每次都冠以新的名称。白宫将倡导'自愿的第三方密匙保管'，将批准'商业密匙第三方保管'，将支持'第三方保管加密标准'，还有将推行'密匙管理基础设施'新计划，随便你怎么叫，它和解码器还是一回事。"

1996 年美国大选期间，因特网保密问题成为双方论战的一个内容。以蒙大拿州共和党参议员康拉德·伯恩斯为首，保守的南达科他州共和党参议员拉里·普莱斯勒、当时的共和党总统候选人罗伯特·多尔、华盛顿州民主党参议员佩里·穆雷以及俄勒冈州民主党参议员罗恩·威顿结为同盟。最初的解码器计划是布什执政时期由国家安全局和联邦调查局共同提出，而由克林顿政

府批准的。现在，康拉德·伯恩斯提出“Pro—CODE”（S. 1276）法案，主张把加密程序的出口控制权既不交给国家安全局，也不交给国务院，而是交给商业部。电子保密信息中心发现这个提议有很大优点，为此在网址上发表新闻公报，宣称这个法案有三项主要原则值得支持：“1、禁止政府把政府设计的加密标准强加于私营部门。2、禁止‘老大哥’开后门进入百姓的计算机系统。3、更新美国外贸加密产品销售的出口控制，使美国企业得以公平地与外国同行相竞争。”根据 Pro - CODE 提案内容，“人们对全球性加密系统的前景的看法正在趋于一致，这一系统允许用户选择任何加密方式，需要时则用备份密匙予以开启。密匙系由计算机用户自愿提供给受信托的一方加以妥善保管。”

1996 年 7 月 12 日，白宫再次表态，正式宣布它反对 Pro - CODE 提案：“这一法案有失偏颇，没有考虑到它允许（加密程序）扩散将造成的严重后果。”总统候选人多尔随即反唇相讥：“克林顿总统所支持的第三方保管密匙方案，只有在政府弄得到密匙或者口令的条件下才许可人们使用强大的加密系统。这使人们油然回忆起（克林顿）政府既官僚又复杂，还无法运作的失败的保健计划。”

加密：世界性对抗

美国所有因特网商业利益集团都同意这样一种说法：他们的世界信息霸权现在岌岌可危。这些公司凭着自身创造力和软件，成为因特网发展的驱动力，它们因而不能理解美国政府为什么要在其加速档上猛扭一把。微软、网景、莲花等公司为了遵守美国出口法规，不得不降低其加密系数质量，他们发觉这是无法忍受的，这使得公司及其客户的生存都受到威胁。这些公司和政府有一点完全一致：无论出于什么理由（兹默曼！），加密再也不仅是政府一家之天下。间谍、外交官和军方不再能够垄断加密术。而且，不管他们多么不情愿，这种历史趋势是不会倒退的。正是因为这个原因，国家安全局才失去冷静。数百万上千万份免费 PGP 软件在传播，在使用，这世界不再是过去的世界。不过，美国是唯一可以合法营销 PGP 的国家。其他任何地方，尤其是古老的欧洲，那里的国家传统有个漫长的演变过程，加密术依然是一个禁忌的话题。欧洲国家，不管是不是欧盟成员，意识深处对加密术都有某种特定的历史框框。当然，PGP 在整个欧洲大陆也广为流传，这要么是钻了法理含混不清的空子，要么就像在法国那样，直接触犯了相关法律。

巴黎早就通过了严厉的反加密法，这无疑是因为军

方和加密干系太深。1986年以前，法国法律明确规定：加密术是一种战争武器。不仅几乎完全禁止出口，也严格禁止在法国本土上使用。那时，使用加密系统就和把坦克开出军营兜风一样困难。1986年2月，当时的法国总理洛朗·法比尤斯第一次试图放宽有关法律限制，但几周之后，他的议会多数就被立法选举推翻了，他本人也下了台，由反对派领导人雅克·希拉克接替。法比尤斯法案的起草人是国防部秘书长。法案表面上没多少变化，但是创立了一个旨在引导法国进入网络时代的特殊机制，即信息系统安全事宜部门间代表团，它使得部分军队和军事人员不得不依赖谍报机构，而且在十年之后的今天仍然如此。这期间，在使用记忆卡的高端银行终端领域里，法国企业家感到出口产品困难重重，对这种法律限制提出了强烈抗议。他们的呼声有了回应：1990年12月，法国通过了一项新的法律，规定："为保证国防、内部安全和国家安全，供应、出口、或使用受益于加密术的工具须受以下限制：1、预先声明其使用或受益除鉴别通讯真伪或确保传输完整之外别无目的。2、其它情况预先经总理授权。"这就是说，如果你为了某项授权给自己的签名加密，没问题；但文件其余部分必须仍然是"透明"的本来面目。这还真是一个进步，因为从前甚至连为授权而进行加密都不允许。不过，假如说法国政府立场有所松动（尽管变化不大），那也不是网上冲浪者施加压力的结果（法国网民在1996年年底

约为15万人，占总人口的百分之二点四)，而是法国企业家长期努力的功劳。企业家们这样做有几个理由：他们希望有能力保障数据安全，但又不愿意眼睁睁地看着美国鲸吞整个加密市场。法国政府末了终于承认企业家们是正确的，但补充了一点：按照有关部门的说法，PGP之类程序遭到了美国家安全局的篡改。当然啦，这么说并没有任何证据。但就是根据这一没有根据的说法，法国政府下令禁止任何法国公司使用PGP，但允许他们用由常年为法国国防部干活的公司在法国设计的程序。起码可以说，那些程序的性能，没有那么可靠。

1996年6月，法国议会通过新的电讯法，其中一个概念正是美国政府所孜孜以求的："信托第三方"——"密匙第三方保管"的又一版本，它可真是网络空间里不断复活的长生鸟。法国法律许可自兹日起，公司和公民个人可以从信托第三方购买程序。不管怎样，每一买主都须同意，有朝一日他们触犯法律时，执法部门有权从信托第三方申领密匙，以便警方掌握犯罪嫌疑人的机密文件。愿意服从这种婚前协议的罪犯恐怕寥寥无几。他们最可能选择的将仍然是不合法的PGP程序。法国政府兜个圈子，又回到了起点。

1996年年底，世界以这样那样的形式，朝着反加密国际立法的方向又挪动了一点点。1996年9月26日，经济合作与发展组织在巴黎专门召开会议，打算就此拟定法案。经合组织还计划于12月16日到20日在巴黎

召开第二次会议。但会议开始的前一天，好斗的加密派就在巴黎举行了反会议，重申他们反对美、法、英限制自由的意图。澳大利亚法官诺曼·瑞伯恩给会议定下基调，怀特费尔德·迪非、麦特·布雷兹、菲尔·兹默曼和罗丝·安德森等活动分子在会上明确表达了自己的立场。他们的发言充满将军在出征前誓师大会上演讲的火药味。

这段时间里发生的一切，似乎都在表明事情已到决定性关头。10月1日和2日，美国又放了一炮，承认白宫和几家最大的信息材料制造商已经结成联盟，从而揭开加密史上的新篇章。这些信息材料绝大多数与硬件有关。美国副总统阿·戈尔[①]10月1日就此发表声明说，这一联盟旨在促进“电子商务和世界范围内充满活力的安全通讯的发展，同时保护公共安全和国家安全。”简言之，加密是好事，但得有条件。更准确点说：“根据这一举措，长度为56比特的加密产品可以经一次性审核后持普通许可证出口，如有变故，依生产和营销支持密匙恢复的未来产品的工业协议而定。这一政策适用于硬件和软件产品。放宽控制时限两年。”制造商必须在两年之内按照新的法律条文调整生产，以适应两年后正式生效的密匙恢复系统标准。到1998年年底，戈尔再次肯定地宣称：“不支持密匙恢复的56比特产品将被禁

① 美国副总统电子邮件地址：vice-president@whitehouse.gov

止出口。”为了确保密匙恢复不致重蹈解码器的覆辙，美国政府许诺就这一概念展开对话：“政府将利用正式机制向企业、用户、国家和地方执法部门以及其他私营部门代表提供机会，就密匙恢复的前景提出意见和建议。主题包括：评估发展中的全球性密匙恢复架构；总结密匙恢复实施中的经验教训；就针对密匙发放途径的技术机密问题提出建议；讨论互操作性和标准问题；指出政府措施中其他技术、政策和程序问题。政府十分同意国家研究委员会最近提出的建议，政府也将研讨有待国会立法的许多事宜。”

戈尔发表声明的次日，美国十家制造商和法国国营的布尔集团公司宣布创建联盟，以“开发可出口的、世界性的、威力强大的加密方法。联盟目标是使各公司有能力进行安全的国际电子商务。”实际上，密匙恢复系统和“第三方密匙保管”唯一的区别在于用户发现失落的密匙的能力，另外执法机构也能够经司法授权恢复密匙。

白宫10月1日发表的公报摘要中，略述了密匙恢复系统的许多特性：密匙最终由用户所在机构内部管理；建立可在国外恢复密匙的国际合作体制——加密引渡形式等等。对政府这一新措施，捍卫公民自由的组织迅速奋起反击。10月3日，民主和技术中心声称，他们不认为“第三方密匙保管”和密匙恢复之间有何区别，而“将‘第三方密匙保管’在全球制度化的企图是

对（美国）国内外因特网用户隐私和安全的根本威胁。”《纽约时报》在一篇引人注目的社论中批评了这一新措施，认为：“还有改进的余地……现在正是同企业和隐私卫士合作，为下一代加密软件解决这些限制的时机。与此同时，政府或许可以推行（国家研究委员会）专家小组提出的其他合理建议，例如在联邦调查局内部开发更好的加密技术，帮助私营部门开发他们需要的防范非法窃听的加密软件。”《华盛顿邮报》认为加密软件从先前的军火级降级一事可庆可贺，但很想知道密匙恢复计划将采取什么形式。该报问道：“这是什么类型的计划？没有人能说清。如果计划不可接受怎么办？两年内许可证还将照旧规定来，到那时安全问题还会不会悬而未决？这是很有可能的。如果不加以澄清，人们就既搞不清楚政府到底有没有妥协或者投降，也不明白政府现在如何看待出口不可破译的软件的危险。”

加密之争的背后，一场更大的战争正风起云涌。在奥威尔式国家信徒和计算机朋客之间展开的这场斗争中，人们指望着能够找到某种现实的中间地带，某种类似于网络民主的东西。在那里，国家作为我们自由的保护神，将允许公民自由通讯，保护他们私生活免遭侵犯。全美上下，不论在鲁比岭还是在大学校园，这场争论一直在扩大，因为人们普遍相信，联邦政府对公民私生活的干预已经太频繁、太深入。

第四章 网上飘飘海盗旗

安东尼－克里斯·兹博拉尔斯基只有22岁，一副老老实实、一本正经的模样，瘦高的个子，蓬松的头发、淘气的黑眼睛，爱开点粗鲁的玩笑，头脑冷静——这和他的经历形成强烈对照。他看上去并不为蹲过监狱而感到狼狈。

兹博拉尔斯基生于1975年，当时个人计算机还没有问世。8岁那年，大人们在圣诞树下给他摆了一台小小汤姆森MO5型计算机。不出几个月，他就深深迷上了这门新技术，开始了计算机探险之旅。那时候，他的小伙伴们还终日粘在电视卡通前面呢。14岁时，兹博拉尔斯基第一次开始重大的黑客行动。1983年，法国刚刚起步搞交互式电话黄页Minitel，他就盯上了电话。兹博拉尔斯基直言不讳地说："我是从非常理论的层次进行的，电话计算机科学就像某种哲学，我思索再三。"

兹博拉尔斯基第一次闯入法国电话网时用的是"税人"的假名，随后又化名"狂人"再次闯入。他在黑客

圈子里闯出了万儿，开始自己创办黑客同志俱乐部，取名为“滥用”（Abuse）。兹博拉尔斯基谙熟英语和法语，而且有一种不寻常的天赋：不管法国人还是美国人，也不管男女老幼，他都能模仿得惟妙惟肖。我问他是否利用某种机器来变换嗓音，他答道：“不，不能那样做，机器声音太冷淡，电话那头的人会立刻感到不舒服。”1992年起，他不再充当好脾气的DIYer[①]，他的名气也传出了他的小圈子。兹博拉尔斯基要“有所作为”了——黑客们用这个词来称呼自己的事业。

嗨，先生，你怎样当上黑客的

黑客天地没有疆界，其中居民都是经过变异的怪物：耳朵粘着电话机，手指尖上长出了计算机键盘。每当绝大多数人沉睡梦乡之时，黑客就睁开了眼睛；系统操作员签字下班和绝大多数办公室关门之际，他们才开始工作。

小小黑客星球里，到底栖息着多少生灵呢？答案是成千上万，其中可能有200位是统御一方的诸侯。这些黑客绝大多数在美国，还有一些在德国、荷兰和法国。

---

① DIYer，DIY即Do-It-Yourself，意即“自己动手”。这个词现在在计算机爱好者中间十分流行。如今是一个标榜自我的时代，人们不满足于使用计算机，还希望自己动手，探讨一下计算机的奥秘。这样做的人，就被称为DIYer。当然，各行各业中都有DIYer。——译者

最棒的欧洲黑客来自斯堪的纳维亚。1996 年 9 月 19 日，北欧黑客曾大显神通，打进了美国中央情报局的网址[①]。中情局在弗吉尼亚州兰利总部的机密倒没有受到打扰。根据最基本的计算机保安措施，中情局电脑除了自己内部联网外，不与任何网络联接，中情局的网站和内部网络是完全脱离的。不管怎样，有时玩笑也能和具体暴力一样造成严重的伤害。北欧黑客在侵入中情局网址时，起初只是要找点乐子，要炫耀他们只凭自己手头微不足道的键盘和计算机，而且得漂洋过海，却可以比世界上最富有、最强大的情报搜集机构更厉害。于是这些小捣蛋们设法进入了中情局网址，更改了网址外貌和每周约有 12 万人访问、但内容平平的《世界情况手册》的功能。黑客们把通常的欢迎信息改写成“欢迎来到中央笨蛋局”；把当时的中情局局长约翰·多伊奇的照片换成了一位无名氏的头像——多伊奇以脾气暴躁闻名，这回必定得大发雷霆；把中情局提供的与其它服务的联接变成“太空新闻”、“裸体女郎”、“停止撒谎”；并全都联上了遥远的、与黑客关系远甚于和美国安全关系的网址。中情局发言人里克·奥伯恩主动承认说：“没有出现任何令我们十分担心的事情。”毫无疑问他说的是事实。不过，通过成千上万的报纸和电视报道，中情局被“黑”的消息传遍了世界各地。

---

① 中情局网址：http://www.odci.gov/CIA/

早先，所有黑客都有个“盗客”（Phreaker）的绰号，即盗用电话线路者，指的是那些利用计算机盗取大电话公司计算机核心的帐目管理系统的进入口令，从而免费使用电话的人。他们或者是通过调制解调器与半个世界之外的同一台计算机保持联系，或者只是和朋友们聊天。有趣的很，一般说来他们彼此从没有见过面，可是多年来相互之间聊起天来滔滔不绝，一天几次，犹如一个虚拟的俱乐部。这些盗客知道怎样进入美国最大的电话局——个人分支电话交换台（PBX），而且随心所欲，为所欲为。他们能够拨打某个特殊的公司电话，拿它当拨打另外一个电话的中继。四处旅行的商人拨打这些电话可以免交旅馆的话费单，从而节省巨额费用。盗客得到这些电话号码后，省的钱甚至更多，被盗用电话号码的公司则要付出高昂的代价。

盗客另外一项有利可图的消遣就是弄到像美国电话电报公司（AT&T）、斯普林特公司（Sprint，美国著名的通讯公司——译者）、法国电信等大公司为顾客设立的电话卡号码和口令。如果黑客得到这样一连串电话卡号码和口令，他或她就可以把电话费分摊在各种电话卡里，从而避免因电话费过多而引起注意。玩这种小把戏创出世界纪录的是迈克斯·劳恩，他于 1994 年 9 月在西班牙马略尔卡岛落入法网，罪名是盗用了 14 万多个电

话卡号码，通过 BBS 黑客[1] 在全美和世界各地出售。通常情况下，这些电话卡以每周 100 美元左右的价格卖给外国移民，他们可以用来在世界任何地方不限时间地通话。黑客每星期都要更新号码，买主可以毫无阻碍地把这些号码转手卖给别人。当然售价不贵，其费用远远低于政府法定费率。

要卖这些号码，首先得把它们搞到手。所以机场里到处是这些盗客。他们在门口荡来荡去，等候商人们走下飞机，走进电话间，用手中的电话卡号码打电话。他们训练有素的眼睛能够在电话卡被塞进话机时读到号码，然后就等着打电话的人输入密码。他们随后离开，回到计算机键盘跟前。即便最警惕的人也会上他们的当。在贝尔研究室工作的亨利·M·克鲁埃普费尔几年前就有过这样的教训。他说："我在一台投币电话机打电话，我挡住号码，不让我左边一个样子邋遢的小伙子看到，但却没有注意到右边那个西服笔挺的家伙。"盗客都有组织。几分钟之内，克鲁埃普费尔的电话卡号码就在美国各地被使用了 600 次，直到贝尔公司的保安人员

---

① BBS 即电子布告栏系统，它和网址的功能相同，但不是通过上网进入，而必须通过一个特殊的电话号码直接拨叫，这个号码往往是不曾被登记的，只有知道号码的"成员"才能够进入该 BBS，在里面浏览信息，下载程序，存放东西让别人来取，以及相互间交换电子邮件。信息黑客常常利用这些 BBS 存储违禁信息，如进入密码、信用卡号码、被"黑"程序等等。

警觉起来，才清除了正在不断扩大的电话灾难。这种形式的电话欺诈会给受害者造成多大损失呢？据美国谍报机构计算，1994年发生的电话欺诈金额达25亿美元，而电讯行业估计在10亿到90亿美元之间。

兹博拉尔斯基另有一套捣鬼办法，即所谓的“社会工程”，他自称是这一行当里世界上最有能耐的专家之一。他给一家又一家企业打电话，打着作为信用卡网络的代表需要核实帐目的幌子，欺骗对方管理人员告诉他当天付费的所有信用卡的号码。然后，他通过电话用这些号码定购计算机设备，并问道：他可以发份传真确认其定单吗？没问题。他就发传真，附一句：“我可以派人取货吗？”接着他自己去拿货，并让他们在电话清单上签字。

1994年1月，兹博拉尔斯基碰上了法律麻烦。虽然他选择牺牲品时一向小心谨慎。他说：“我甚至会给他们中的某个人打电话，和他谈谈有关情况。那家伙说我从他的信用卡上弄走了2000美元，但这不是什么问题，保险公司会赔偿。不管怎么样，我只选择真正的大公司下手。”听兹博拉尔斯基讲话，你会觉得什么都能从电话里弄到：美国运通卡号码和密码、计算机口令、电话卡等等等等。比起这位年轻黑客的所作所为来，唯一更值得注意的就是他的受害者们多么轻信，多么容易受骗上当。

兹博拉尔斯基和他的一帮伙伴曾略施巧计，不费分

文就举行了一次 15 位黑客的电话会议。他们为此利用了美国电话电报公司的“联盟”系统——许多跨国公司都用这个系统进行内部磋商。这些黑客先是在美国打电话，所拨号码可以联系上所有与会黑客。但参加会的人不用分别掏钱，而是由公司一次付清。和所有电话单一样，许多号码是彼此相似的，只不过这儿或那儿有一位数字不同，所以稍加实验很容易就发现其它的号码。

对兹博拉尔斯基来说，从法国向美国拨电话，而且使机器相信电话是从美国国内打来的，这只是小孩子的把戏。他从一家电话交换台跳到另一家电话交换台，发现了无数电话会议号码，其中一个竟然是属于美国联邦调查局的。兹博拉尔斯基紧跟着就向美国驻巴黎大使馆打电话，得知联邦调查局驻巴黎反谍报主管官员的姓名是托马斯·贝克。“我就对自己说，这个机构那么大，他们永远都不会留意到。事实上，他们问都没有问过。当我下决心要干什么事，我总有把握能干成……”接着，兹博拉尔斯基就得假装成贝克骗过联邦调查局美国办公室的一位秘书“帕翠西亚”，从而得到一些电话号码。联邦调查局最后还是发觉了兹博拉尔斯基的非凡成就，那是因为有一天他又假装成贝克打电话以便通过检查时，贝克本人正巧就坐在隔壁办公室里。

当然，事态急转直下。联邦调查局估计自己损失了约 25 万美元，恼羞成怒地起诉兹博拉尔斯基。1995 年 4 月 10 日，兹博拉尔斯基被暂时监禁，又回到了监狱。

此前他曾因在信用卡上玩把戏而在法国默伦坐过牢，这回宪兵又在那里等着抓他了。兹博拉尔斯基很快就出了监狱，但等着他的是新的审判。1997 年 2 月 25 日，兹博拉尔斯基发觉自己站在了巴黎第十二巡回法庭面前，不得不向法庭解释他为何“道德感”如此薄弱。他的计算机反文化理论没能打动法庭，法庭对他十分严厉，不仅勒令他按联邦调查局所要求金额如数赔偿，而且判他缓刑。但兹博拉尔斯基从此洗心革面，写了一本书，于 1997 年秋天出版。他还和所有自视甚高的黑客一样，自己创办了一家计算机安全公司，取名“免疫”。显然，世俗智慧在网络空间也很适用：如果你不想被偷，雇个小偷教你怎么做。

盗客、黑客、骇客?

疯狂的盗客也是黑客中的一员。他们在闯入远程计算机时，用的是最尖端的技术。在网络空间，盗客、黑客（Hacker）、骇客（Cracker）这些词的涵义虽然论差别很是微妙，但也各有所指。盗客专闯电话系统。盗客圈子里名气最大的是“克伦奇船长”约翰·德雷珀。他曾发现用一个 2，600Hz 的信号就能进入美国电话电报公司的计算机内部管理系统。盗客们还测算出一枚 25 美分硬币投入投币孔的频率，并找到产生和导入这个频率的办法，藉此蒙骗付费电话以为是在“鲸吞”25 美

分的硬币。从技术上说，盗客的电话黑客行为远比黑客的初级。如果说盗客是商店里偷无糖口香糖的小贼，黑客就是偷法拉利汽车的大盗。黑客闯入计算机系统通常都没有恶意——他们是在比武竞技。才华横溢的计算机科学家的大脑胜过最复杂的微处理器。他们的娱乐就是钻进壁垒森严的系统里看看里面的东西，很有点像游客踱进某栋历史建筑或者博物馆参观。假如他们偶然复制走一个程序或者什么信息，他们认为这不算偷盗，而是与之分享，是从礼品商店里买纪念品留念。

黑客常常进行洞穴式探险，深入到巨型计算机的心脏。这些巨型计算机里隐藏着秘密服务器，秘密服务器所在的计算机区域难得被访问，内中存有违禁信息（例如，用于巧妙地越过保安系统的软件，或者色情资料的服务器）。黑客们借助于部分大学或科研单位的计算机，能够存取远超过他们承受能力的内存，而且不需要冒在他们个人硬盘上储存非法资料的风险。这些计算机中许多都不直接与因特网相连，但他们通过一条特别线路拨号，就能直接访问这些材料。联邦调查局断定，这类计算机中能够上网的，将近百分之八十都是黑客在联接。

黑客中的败类就常常被称为骇客。他们总是尽量干坏事：清除文件、安设“逻辑炸弹”。当然其中更有坏蛋，阴谋破坏所在公司的计算机，如此等等。

在 USENET 网中，黑客们交换着各种诀窍和公式；秘密的 BBS 在大量繁衍；到处都是简单涉及或者直接

谈论黑客行为的新闻组[1]。各种高度活跃的邮件列表向黑客们通报着这一领域的最新消息，这和他们的对手每天收到的黑客活动通报很有点儿相似[2]。网上还能看到专门为黑客服务的杂志，如《Phrack》和《2600》。这类杂志有些可以在报摊买到，有些可以订购，但有些——如《计算机地下文摘》[3]（CUD）——则只有网上才能看到。黑客并不只是一群令人喜爱的寻求刺激的青少年。美国有个自称“因特网解放阵线”（简称 ILF）的团体，可能是“骗术大师”（Masters of Deception）或“末日军团”（Legion of Doom）的旁支，专门投递邮件炸弹或者被称作“火焰”的数量庞大、内容淫猥、充满威胁的邮件，直至把受到袭击的倒霉的记者的电子信箱淹没和冲垮。

末日军团成立于 80 年代，是美国最有名的黑客团体之一，其名字来自卡通英雄超人的最凶恶的敌手。末日军团的领袖是位精通电讯系统的计算机专家，化名——或用黑客的行话“头衔”——是莱克斯·鲁瑟。后来，得克萨斯州的克里斯·乔根斯（又名血斧埃里克）和几位末日军团成员在 1990 年时受到了谍报机构的调查，但无论乔根斯还是其它在得克萨斯活动的末日军团

---

① 有关新闻组的网址：alt.2600，alt.hacking，或 alt.cyberpunk.tech

② 有关新闻组的网址：alt.security，comp.security.misc，misc.security 等等。

③ 欲订阅者请发电子邮件至：LISTSER@VMD.CSO.UIUC.EDU

成员都从没有遭到过起诉。末日军团自创建时起就是黑客世界的主角，其成员隐姓埋名，凭着野性未驯的心智和谙熟的技术在黑客帝国纵横驰骋，每每把国内外追“黑”族惊得目瞪口呆。他们的所作所为都在其秘密通报《末日军团技术杂志》中留下佐证。80年代末，末日军团迅速成为美国黑客情报的参照，以至于负责调查他们的警察相当公正地假定：只要网络空间里发生了什么严重事故，这些家伙就应当负责。

从那时起，黑客就在美国人的集体意识中占据了一个独特的位置。把他们抬到民间英雄的位置还欠火候，但他们确实具体体现出某种世纪末的前卫价值观，而这种价值观又和美国赖以立国的浪漫理念相一致。斯蒂芬·列维在《黑客：计算机革命的英雄》一书中指出：“黑客相信，分解系统，观察它们如何工作，并利用这种知识创造新的、甚至更有趣味的东西，从中能够学到的基本经验教训不仅和这些系统有关，也和世界息息相关。他们憎恨任何试图阻止他们这样干的人、物以及法律。”和探险家一样，黑客对自己的发现抱有极大的热情，公布这些发现也是为了和他们一样热情的听众。不过黑客圈子里没有不变的忠诚，常常会发生冲突，例如末日军团和骗术大师之间的战争。这场战争好比某些中世纪小说的翻版，里面也有英雄和恶棍、地主和仆从，最后还有牺牲者。基本经过是这样的：骗术大师决定炫耀一回实力，而从前在末日军团干过的几位黑客目睹骗术大师

华而不实的表演，打算给他们一点颜色看。起先，骗术大师计划攻击克里斯·乔根斯和另外两位末日军团成员在1991年创办的Comsec计算机安全公司。乔根斯和他的合伙人都认为这太过分了，便决定设立某种网络空间的社区监督来保护网络，通过它追踪骗术大师并控制他们。乔根斯声称，Comsec公司给过骗术大师所有平息事态的机会，最后才把搜集来的证据送交电话公司的安全部门以及联邦调查局和谍报机构。骗术大师则说，Comsec英雄们的行径不是网络空间里什么勇敢的自治警察行动，而是一次带有种族歧视动机的袭击（Comsec公司成员是南方白人，而骗术大师成员多半不是）。这很难得到证实。据报道，有一天，血斧埃里克（即克里斯·乔根斯）向菲伯·奥普梯克（即马克·阿伯尼）发送了一份末日军团T恤衫广告，收到的答复是一封死亡威胁信，写信人向血斧埃里克保证他参加一个即将召开的计算机安全会议后，唯一可能的回家方式就是被装在尸体袋里。骗术大师成员被指控的罪名有些非常严重，包括从公共电话网窃听电话交谈、窃听数据传输、截取数据传输、拥有计算机黑客硬件和软件设备、偷窃口令、出售口令、偷窃信用档案、出售信用档案、摧毁计算机系统并造成37万美元的损失。除一次外，这些年青黑客还没有从恶作剧中赚到过一分钱，但却受到严厉的惩罚。1993年，保罗·斯蒂拉和埃利阿斯·拉多泡罗斯在联邦监狱服刑半年，又在家中软禁半年。约翰·李被判

一年监禁、三年狱外监督和200小时社区服务。朱利奥·费南德斯同意出庭指证马克·阿伯尼，被判缓刑。他们当中水平最高的马克·阿伯尼被判刑一年。

毫无疑问，克里斯·乔根斯是黑客天地里最重要的角色之一。谣传说，他曾成功地制造了几起颇为壮观的黑客事件，但从来没有被抓住过。他还是办得十分成功的《Phrack》杂志备受尊敬的主编。这本杂志在黑客圈子里蒙有一层神话色彩，堪称全世界所有计算机犯罪者的网上圣经。它是敬畏上帝的老实人的克星，是传播炸弹配方、交易黑客工具以及提供破解和进入远程计算机方法的自动售货机。《Phrack》杂志不仅让世界各个角落里的网络警察神经战栗，也恰到好处地把握住了黑客世界的脉搏。克里斯·乔根斯白天上班，一到晚上——每天晚上，他拿出一个小时的时间浏览来自世界各地的电子邮件。他说："有电的地方就有邮件，从俄罗斯，从亚洲，我都收到电子邮件。每星期有600封……"乔根斯原先穿着褪色的牛仔裤，蓄着长长的头发，加上其它装饰，一副反文化的"酷"样子。随着时间的流逝，他的装束也在渐渐改变。1995年秋天我遇到他时，乔根斯已创办计算机安全公司。当时他穿一身漂亮的套装，里面一件无可挑剔的干净衬衫。他转过头来时，当然啦，那垂到腰部、扎成马尾的长发还在发出警告：此人没有完全接受现行体制。一年后的乔根斯坐在华盛顿特区一家宾馆豪华的休息室里，灼灼有神的眼睛一如既

往地充满着活力，但头发却剪短了。

好医生乔根斯有两副面孔，一面被他藏了起来。如果血斧先生还活着，他就活在乔根斯大脑皮层的另一块地方。1996年9月底，乔根斯编完第48号《Phrack》杂志。这一期内容包罗了人们能够指望的所有有关黑客策略的情况，还有他的最后一篇社论。乔根斯借这篇社论告别了黑客天地。他不再像从前那样摆出一副网络武士的姿态，而是提出了在第一代黑客中屡见不鲜的一个观点，即对复杂的计算机技术的欣赏以及攻克难关的竞技精神现在消失了，这些最重要的美德比起不光彩的目的来已退居第二位。乔根斯由此态度鲜明地总结了他对过去和未来的黑客行动的看法："我不喜欢你们中间的大多数人。黑客亚文化已经成为对它的过去的嘲弄。人们可能会辩解说，黑客社会在'演变'或者'成长'什么的，但那全是废话。黑客社会在退化，它已成为传媒起哄的闹剧。曾几何时，黑客行动代表着一门依靠智力探求发现的艺术，现在却被一种贪婪、自高自大和放错地方的后青春期焦虑情结所取代……看来'黑客行动'已变成许多人为反抗'某桩事'而寻求出路的下一个合乎逻辑的步骤：'喊！我已经给身体每寸能够刺上的皮肤刺了青，把头发染成了蓝色……到底现在我还能干些啥震一震老爸老妈？我知道了！我得犯法，或者还能把名字登到报纸上！那该有多酷！就像电影里一样！'我讨厌戳穿任何人的肥皂泡，但你们错得一塌糊涂。在今天

这个时代，当一名黑客根本不需要干非法的勾当。现在任何人都有很好的条件合法地学习到更多的东西，使用更强大的计算机。70 年代末和 80 年代初的时候，我们所有人连梦都没有梦到过这么强大的计算机。我们那时候，完全是在学习怎样使用这种被叫做计算机的怪物。”写下这篇社论数周后，乔根斯进一步解释道：“如今，没有人非得采取违法手段来学什么不可，那个时代已划上了句号。在过去某个特定历史时期，唯一的学习办法是窃取访问方式。但今天你能够随心所欲地把更加强大的操作系统下载到家里的个人计算机上，这是我们 15 年前从来做不到的。如今不存在非法闯入的需要了。现在闯入某个计算机系统的唯一报偿要么是窃取业主的信息，要么就是因为明知在干坏事而享受到高度刺激。这不是我们那时搞黑客行动的目的；但十分不幸，现在看来黑客们孜孜以求的却正是这种东西。现在的黑客不是‘叛逆’，他们是在东施效颦，是在搞些高科技的哑剧，其中原创的意义多年以前就消逝了。”

对乔根斯来说，早期黑客的“叛逆意识”和新生代之间的冲突不应该对任何人构成严重问题。一段时间以来，他改弦更张，遵纪守法，事事以美国利益为第一，而且不乏同道者。在 1995 年 11 月罗伯特·斯蒂勒发起的开放源解决办法会议上，我注意到了这一点。斯蒂勒曾经是中情局和海军陆战队的特工，是第一位认真对待黑客并且认识到黑客对情报界的贡献的人。这很不容

易，因为所有地方的商界对黑客仍然望而生畏。斯蒂勒自认为是黑客和情报机构—— 在更大范围内，还有国防部门——之间的桥梁。于是，11 月份一个寒冷的下午，在华盛顿特区奥姆尼·肖汉姆宾馆，世界上最令人难忘的四大黑客高手就坐在了我们面前（凯文·米特尼克不在场，他从上年 2 月就被关进了威克县的联邦监狱）。黑客们审视着他们面前的听众：几十位美国企业界头面人物、各情报搜集部门负责人以及其他五角大楼的高级官员。所有与会者都如坐针毡。

四大黑客中，和克里斯·乔根斯坐在一起的是达克·谭简特，朋友们称他为杰夫·摩斯。值得一提的是，达克·谭简特是世界上最疯狂的大会——唯有黑客才能参加的 Defcon 黑客大会的组织者。这天下午，在华盛顿，身边坐着凶神恶煞似的同行，埃里克·休斯则如身登极乐世界一般飘飘然。休斯一把红胡子，头发甚至比乔根斯的还长。他住在加利福尼亚州柏克莱，日子过得懒懒散散，但却是加密朋客的开山祖师，世界上最厉害的计算机科学家之一。他兼网络自由派和数学家于一身，但把前一个身份看得更加重要。在自由和网上个人自由不受限制的旗帜下，他与他的门徒并肩作战。休斯生活中真正热衷的是两件事：破译脆弱系统的密码和编写出让政府的‘密码分析家们’不知所措、拱手求饶的密码。黑客四重奏里的最后一位是黑色头发、面容忧郁的伊曼纽尔·葛德斯滕，他是盗客杂志《2600》的负责人。为

何取名2600？因为在黑客的冰河时代，把一个25美分硬币迅速投入付费电话的投币孔所产生的频率恰好是这个数字。黑客前辈克伦奇船长的这个小小发现让黑客们免付了好多年的电话费。

四大黑客为何会出席这次信息会议呢？首先要知道，他们是正派人，正派的美国人，愿意加入信息战争，为避免许多军事官员所恐惧的电子珍珠港事件出力。开放源解决办法公司负责人罗伯特·斯蒂勒在会议开始时向350名与会者作了简要致辞。他说："是的，我们邀请了一些黑客。他们胡子拉茬，不修边幅，不到中午从来不起床。但他们是非传统型战士，美国需要他们。他们中有些人应当被打屁股，但他们也应当有机会陈说国王没穿衣服的真理。他们是美国最可宝贵的国家资源之一！"一年之后，斯蒂勒再次肯定地说："我最初认定黑客需要和最高级政府官员公开对话是在1992年，当时我认识到……我们的通讯和计算机化基础设施非常脆弱和容易被摧毁。为着一个愚蠢的原因——恐惧，这种情况在大多数国家被当成头号机密。黑客就像宇航员一样，充满'恰当的素质'，不停地开拓着网络空间的边疆——我们可以从他们那里学到很多东西。"

不过，黑客从前养成的习气容易根除吗？指望他们从绿林强盗摇身一变成为爱国者是否太过奢求？乔根斯向一位全神贯注的听众解释说："黑客不是强盗。他们做事情是为了寻求乐趣，而不是要从中牟利。他们想进

入一个系统，在一堵虚拟的墙上写下：‘我到此一游，’然后通知网络管理员。无论如何，真正的强盗不是十几岁的青少年。尤尼克斯操作系统的工程师能干得一样出色，那儿才应该是你们找罪犯的地方。”在会议室里，每个人额头都冒汗了。乔根斯继续说道：“日本人和法国人渴望从你们的系统中窃取情报，我们就没有那么在乎。我们黑客没有钱，而他们有，能够用钱买到他们想要的所有情报。”老实说，乔根斯的经济窘况也成往事。现在他成了一杆出租的枪：各种公司掏钱雇他闯入公司计算机系统，然后把他发现的漏洞给堵上。在会议室，一位面色红润的将军举手提问：“我们知道自己有弱点，应该怎么做才能防范海盗行为?”达克·谭简特锐利的眼睛盯住将军：“封闭一切，加密所有的东西——回叫信号、传真、电话、电子邮件。不要公开任何东西。而且，使用移动电话就和在大庭广众面前发表演说一样。”乔根斯插话说：“关闭电子门，监视因特网，里外都要监视。”将军坐回座位，看上去十分无助。一位商人问道：“你们对防火墙怎么看?”黑客们互相看看，露出开朗的微笑。一位黑客问：“自己盖的吗?”“不，但我有一个。”“噢，这样。你得确保使用的是动态的口令或口令段。它们应当可以随机产生而且应当不断改变。”房间里静得绣花针掉在地上都听得见。

世异时移，坏男孩现在改邪归正了。但是，事情当然没有这么简单。许多人都反对这么轻易就提供给黑客

功成名就的机遇。1995年9月在华盛顿特区召开信息战会议后，计算机安全顾问多恩·B·帕克就轻蔑地谈到向黑客提供布道讲坛的主张："存心不良的黑客是我们的敌人，是证据确凿的罪犯或者罪犯的支持者，他们不是我们的朋友。只有异想天开的人才认为如果他们作为朋友对信息所有者和他们脆弱的系统进行可恶的攻击，他们也能得到重视……当黑客是个白日梦，是在走捷径取得你们所制造和鼓励着的成功。这意味着你们在引诱年轻的、充满潜力的信息技术人员成为心怀恶意的黑客，选择死路一条的堕落的生活。"全美计算机安全协会（NCSA）会长彼得·S·梯派特是会议的组织者之一。他觉得，完全可以期望和尊重向黑客提供一个讲话的地方的做法。他说："各种因素中，对真正的威胁缺乏真正的理解，造成彼此合作的各信息安全部门里所有的资源盗用现象（例如为了64比特对128比特密匙忧心忡忡，同时却任凭各种谎言、欺骗、偷盗、默许或者共同的虚张声势、黑客较技、团伙图谋等等大肆进攻）。缺乏理解还导致所有各种猜想、臆测，甚至还有些无疑是误导了的关于黑客的正面传说纷纷出笼。"

不论你从哪个角度看这个问题，无论如何，负责管理大公司内部信息网络的少数系统工程师尚无能力抵御黑客，保护自己。因此，黑客的攻击意味着计算机操作员得通宵不眠，有的甚至还得匆匆设定小程序来自动通过BP机呼叫自己。黑客入侵中央计算机时，不管是不

是在真正破关闯入之前，往往都利用用户的懒惰——安保系统所要求的严格和那些有备而来的黑客的松弛不可同日而语。安保系统的薄弱环节之一是对最常用口令的管理太过初级，使得专门用来产生和插入各种口令的软件很容易就找到它们。目前为破解更复杂的口令而设计的其它程序有：Crack，Shrack，Crackerjack，Cracklib，Npasswd，HaughII 等等。

各种政府安全部门使用的程序甚至威力更大，其中许多都是美国公司 Accessdata、WR Pass 和 MS Word 生产的。像"警察"（COPS）和"撒旦"（SATAN）这类安全软件所使用的系统其整合性非常强，实际上倒对黑客十分有用，因为破译代码的模块早已整合进程序中了。把一种又一种语言中最普通的单词（专有名词和普通名词）输进去，他们就能够逐渐地、一点一点地清除假定能防范黑客侵袭的计算机防火墙。

所有自视甚高的黑客都不时地使用各种口令字典[①]，但他们可以使用诸如"古滕贝格"（Gutenberg）这种包括虚拟书架的数据库[②]，轻而易举地自行编辑这类字典。至今我们还没有遇到哪位黑客因为口令而明显慢下来过。如果女人的名字、著名街道或城市的名字都不对，韦伯斯特大字典的某处总该有每个可以想象得到的

---

① 参考网址：ftp：//cdrom.com：/pub/security/coast/dict/wordlist

② 参考网址：www.promo.net/pg/

变字。如果计算机加以拒绝（试错三次后计算机通常会自动切断连接），黑客的系统将自动重拨，需要的话可连拨几个小时，直到找到办法进入。黑客经常使用一种在下载被攻击计算机的口令管理文件之前克服一系列障碍、防火墙和动态口令的技术，它可以使黑客坐在家里发出攻击，爱用多长时间就用多长时间，而且不必冒被机器拒绝和引起注意的风险。假使一名优秀的骇客能够每秒运行约五万个口令来通过这样一个管理文件，这看来是最好的办法。

尖端计算机信息保护人员早已设计出不少用于商业销售的软件，如防火墙1号、Sidewinder、Gauntlet、Raptor，以及最广为人知的BorderWare（过去称为JANUS）。不过，这些盾牌式软件起的作用似乎只是吸引黑客骑士用更长、更有力的矛去刺穿它。有个时期美国军方十分着迷这类东西，相信唯一切实的反渗透办法就是在系统内引进从用户登录时起就追踪用户动向的程序。那么怎么防止黑客进入呢？可能通过增加和增高黑客所需跨越的障碍，只有攻克人们能够想象出的最森严的计算机壁垒，才可以接触到最敏感的信息。

“撒旦”是个好东西

对丹·法默和韦埃斯特·韦诺玛，黑客怎么夸赞也不为过。这两人是最强大的黑客程序“撒旦”的编制者。

这个程序全称是分析网络安全管理工具，首字母缩写为SATAN——魔鬼撒旦。数年来，“撒旦”早已在系统管理员中间扬威立万，系统管理员们靠它发现系统的薄弱之处，这是保护系统的更好的方式。“撒旦”的创新不限于其技术的精湛高妙。为了向盘踞网络空间的众多邪恶势力更清楚地表明这一点，经过大规模舆论宣传后，“撒旦”于1995年4月5日在因特网上发布，随即引起一片恐慌：“撒旦”把黑客和反黑客人士都同样武装起来，而双方兵戎相见之后，显然都对“撒旦”备感满意。丹·法默在完善“撒旦”程序时，还负责加利福尼亚州最有名气的软件公司之一硅图像公司（Silicon Graphics）的安保工作。法默没有选择国家安全局，虽然后者也曾发出邀请，但后来此事落进官僚主义的乱麻当中不了了之。

有三年多时间，丹·法默一有空就考虑综合一种方法，以便加强对雇主信息安全的保障。随着想法的逐渐明朗，他在软件中使用了引人注目的图形界面。“撒旦”与国家超级计算机应用中心设计的马赛克浏览器十分相似，完全不懂计算机的人也很容易上手，加上它发现系统弱点的速度，使得这个软件成为黑客无可挑剔的工具。黑客们再也不需要高深的专业水准，也不必再花费昂贵的上网时间磨练技术了。

硅图像公司相信法默的软件会毁坏公司的声誉，他们宁愿把它专门保留给那些希望得到安全保障的公司使

用，因此想禁止在网上发布它。但这不是法默的选择。1995 年 3 月 1 日，法默在记者招待会上表明了自己的立场，他承认，从某一点上说，“撒旦”确实会带来危害。但他的选择符合他的生活方式。他说：“我是一个双性恋者。我既是性虐待狂也是性受虐狂。我从事安全工作，我爱喝上好的葡萄酒。我为什么要隐瞒呢？那一套应该把不正常的东西藏着掖着的说法真让我恶心。”尽管法默提倡负责地使用“撒旦”软件，他仍旧被公司炒了鱿鱼。

随着有关新闻报道开始出现，越来越多的人知道了“撒旦”的存在，恐慌情绪遍及网络空间。程序员打开的门怎么关上？又怎么阻止那些铁石心肠的黑客——他们要么专去不该去的地方，要么以偷窃软件为乐，要么把程序员和公司都推到灾难的边缘。

面对这些计算机灾难，公司所能找到的最好的盾牌自然就是投诚的黑客。他们也利用专门的因特网新闻组来交换偷盗技术，试验他们制作的各种防火墙。如果你想订购有关各种邮件列表，那你每天都会收到多达一百封的电子邮件信息。黑客和反黑客虽然不总能完全说清他们各自站在哪一边，但他们知己知彼，你争我夺，互不相让。

所有这一切中，最让人吃惊的是速度——消息传播、逆命令下达和错误发现的速度。1995 年 4 月 5 日开始，在国防高级研究项目局支持下，匹兹堡卡内基－梅

隆大学成立了计算机紧急反应小组（该小组至今仍接受政府资助），并在网上以洪水般的规模大量发布了COPS程序。COPS程序也是丹·法默设计的，能够帮助抵御“撒旦”的侵袭）。同一天，劳伦斯·利弗莫尔实验室宣布它的COURTNEY程序也具有相同功能，并在服务器上提供了“撒旦”程序——它立刻就被复制了1500份。

黑客定期举行的集会向来令人好奇。1995年6月2日，《Phrack》杂志在亚特兰大召开年会“夏季会议”。这回会议不再保密，而且通过因特网向所有人——“黑客、盗客、盗版专家、病毒制作者、系统管理员、执法官员、新嬉皮士、特工、教师、满腹牢骚的雇员、电话公司走狗、纽约客、程序员、阴谋家、音乐家和裸体主义者”发出邀请。邀请信上清楚地阐明了游戏规则：“我们的一贯主张是：通过开会促进社会交往。除开私下场合，‘秘密黑客信息’从未被真正讨论过，因此人们只有结交新相识，主动展开饶有趣味的讨论，才能了解黑客情况……夏季会议的正式演讲部分将只举办一天，而不是两三天，让人们有充分的时间在城里游历，切磋黑客技术，搞搞破坏，或者和他们至今没见过面的网上朋友聊天。”如今在这种形式的会议上，黑客、联邦调查局人员、各种谍报机构特工以及防火墙程序员鱼龙混杂，已经是司空见惯的事情了。

你搭墙，他来拆

凯文·米特尼克曾经以为，这样的日子永远都不会结束。多年来，这位黑客王子在网上游荡，从来没受过惩罚。没有什么在他面前能保住密，他可以进入任何一台计算机。不管系统设计得多么严谨或者号称针插不进、水泼不入，他总有办法要么在电子篱笆上找个洞钻进去，要么弄根合适的电子撬棍完成任务。米特尼克乃是一位信息渗透艺术大师。不过，1995 年 2 月 15 日，多年一帆风顺的米特尼克一下子就突然遭遇巨浪滔天的汪洋，原因很简单：他忘乎所以了。

米特尼克被捕后，司法部发言人约翰·罗塞尔把他称为“信息恐怖主义者”。事实果真如此吗？似乎有些夸张了。与其说米特尼克是枚疯狂的炸弹，不如说更像一位后现代、高科技的罗宾汉。但是，不管怎样，米特尼克在他的十年秘密活动中还是搞了一些破坏的。1981 年，年仅 17 岁的米特尼克就利用计算机设法从太平洋贝尔公司中央计算机里复制了密匙资料，并因此受到当局追捕。他还和朋友们首先成功地闯入了负责保卫美国和加拿大领空的北美空中防务指挥系统。这场小闹剧甚至吸引了好莱坞的注意，好莱坞把这个情节用到了电影《战争游戏》里。八年之后，米特尼克闯进数字计算机公司，据该公司估算造成了一百万美元损失，米特尼克

为此蹲了一年监狱，并因为行为困难而接受心理治疗。

这时的米特尼克在黑客中已享有神话般的地位。1992年11月，他逃之夭夭，彻底从万丈红尘中消失；逃得谍报机构和私家侦探连一点蛛丝马迹都找不到。一段时间里，谁都没有他的消息，他比以往任何时候都更加难以接近。这时他策划了另一起攻击行动，目标是一家甚至更为重要的金融机构。米特尼克不再满足于仅仅闯入公司计算机系统，从某位在线服务商客户数据库里盗取所有信用卡号码之类的东西——仅在圣何西的 Netcom 里就有两万信用卡号码；他也不想再解构令他苦恼的一些攻击路线。他现在进攻的是个人的私敌。有一次，他把一家医院三万美元的电话帐单转给了他的一位亲戚。另一次恶作剧里，他把打给某大公司交换台的电话全都传递到一条私人线路上，这条线路于是被没完没了的电话洪水所淹没。

但米特尼克也有他的致命弱点，就是骄傲。他决定拿老朋友下村勉开刀。下村勉是世上唯一和米特尼克技术水平旗鼓相当的专家。不久以前，他就和米特尼克一样令人畏惧，现在下村勉向那些希望防范黑客袭击的企业和个人提供有偿服务。

事情出在1994年圣诞节早上。下村勉刚要吃圣诞节火腿，就发觉有名黑客设法闯入他的计算机，想要复制点奇迹。下村勉采取了非常严厉的对策。几个小时之后，主要上网服务商“全球电子连接”公司（WELL）

打电话给用户布鲁斯·柯伯尔，通知他他的上网帐号活动表现异常。柯伯尔十分惊愕，他检查机器内部情况后发现，千真万确，在过去几天里，机器出现异常运行。更仔细地审视之后，他看到他机器持续呼叫的计算机中有一台正属于下村勉。原因如下：米特尼克为了匿名闯入下村勉的计算机，通过调制解调器访问了许多人的机器，并且在业主不知情的情况下把这些机器作为中继。访问密匙和口令都是从服务商处偷来，之所以选择柯伯尔既是因为他上机次数有限，也因为他是一家名叫“计算机、自由和隐私”的计算机信息智囊组织的负责人。该组织的年会很受欢迎。在其 1994 年芝加哥年会上，联邦调查局曾经突然闯进会场，逮捕了一个长得很像米特尼克的人……随即又释放了。

“全球电子连接”在网络空间是一座纪念碑。下村勉和电子边疆基金会都信奉网络自由，他认为米特尼克的小把戏一点都不好笑。所以，“全球电子连接”的成员经过投票后决定向联邦调查局告发。这是个困难的决定，特别是因为“全球电子连接”长期以来一直对黑客提供帮助，通过网络接纳了形形色色的计算机信息自由派。但这次事件不同，米特尼克做得太过火了，触犯了太多忌讳。他对下村勉的攻击超过所能容忍的界限，使下村勉深深受到伤害。下村勉是圣迭戈超级计算机中心的高级科学家。这家中心办得非常成功，以至于国家安全局也找上门来（对一名前黑客来说，这是莫大的成

就），要求它帮助建立一套超大范围的监视系统。于是，米特尼克闯入的整个过程都被分解成微小详尽的细节，他每次闯入的路线被一一确定，他对其他计算机的攻击被系统地重建，他的策略所受检查之严格，换他本人来做也不过如此——这没什么新鲜的，最优秀的计算机反间谍专家一直就是最优秀的间谍。下村勉把范围缩小到查找米特尼克如何进入 Netcom 的，并让联邦调查局监视这家公司。尽管米特尼克诡计多端，他的拨号源最后还是被找到了：这些号码全都来自位于加利福尼亚州北部的罗利，能够确定这座城市还得归功于米特尼克使用的移动电话中继。

1995 年 2 月 15 日中午一点半，联邦调查局按响了米特尼克家的门铃。几天后，热心维护加密术的布鲁斯·柯伯尔评论说："具有讽刺意义的是，政府在动用一切力量追捕米特尼克的同时，又把时间耗费在压制能够保障网络安全的技术上。"柯伯尔补充说道："杰迪骑士（电影《星球大战》主角——译者）投向了黑暗的势力。"下村勉赢了。很久以前，国家安全局就在召唤他，现在他可以回去工作，国家安全局还邀请了下村勉的朋友、"撒旦"发明者丹·法默，但后者没有贸然答应。全世界第一流的黑客和全世界第一流的情报搜集组织联手合作，而这位黑客的铁哥们儿编制出的程序，就好比一柄可攻可守的双刃剑一样棒。

米特尼克成为反英雄，一匹害群之马。末了，他甚

至没有从这些行为中弄到多少钱。米特尼克被送进威克县监狱，受到的限制和其他任何美国罪犯都不同：他被禁止打电话。监狱管理人员在和下村勉谈过后，认定该犯能够利用其特长消除犯罪证据（这些罪证可能甚至过分地树立了他的技术威信）。服刑期间，米特尼克只获准和他母亲和祖母通话，而且由看守亲自动手拨电话号码。

那么，凯文·米特尼克到底是何许人也？他是政府想让我们相信的那种对社会心存敌意的人吗？抑或如克里斯·乔根斯所言：从来没能摆脱青春期而成熟起来？可能真正的答案比这些都更加错综复杂。1991年，凯蒂·哈夫纳和约翰·马考夫合写了一本关于计算机黑客的书，在为此书写刊后语时，她拜访了一家犹太感化院的院长哈瑞埃特·罗塞托——1989年米特尼克因其它事坐牢，出狱后曾在该院住了几个月。这位社会工作者对米特尼克的看法很有意思，她相信米特尼克是“一种毒瘾”的受害者。她说：“和米特尼克的沉溺行为最接近的，就是赌博，既不为挣钱也不为输赢，而是对这么做上了瘾。”米特尼克被捕之后紧跟着出版的两本书也对这种疯狂症候提供了引人入胜的资料。第一本是下村勉和约翰·马考夫合写的著作，从猎手的角度详细描述了铁石心肠的猎人追踪逃犯的情形。著书者——猎手不捕到猎物决不甘休。下村勉在书末解释了他愿意透露这么多细节的原因。他说：“对我来说，他（米特尼克）真

正的罪行是违背了原始的黑客道德。阅读他人邮件是不正当的。相信人们应该自由地共享软件和计算机技术是一回事，相信可以去偷盗它们是另一回事。”

黑客们往往认为第二本书更加全面和善解人意。该书作者约翰森·利特曼在米特尼克躲藏期间和他有过联系。利特曼相信：“神鹰”——米特尼克在网络空间的绰号——是遭到陷害才跌了这么一跤，而且在一定程度上联邦调查局有人插手。该书详细叙述了米特尼克的神奇经历和他与莱维斯·德佩尼的友谊，后者是米特尼克与外间世界的唯一联系。身为曾遭到美国司法部最猛烈的通缉的前黑客，凯文·米特尼克以后会怎么样呢？1996年9月26日，美国司法部在圣迭戈对米特尼克提起25项重罪起诉，看来他摆脱法律困境的日子远着呢[①]。

知识产权……为偷为盗

人人自危。1994年10月，黑客设法闯入佛罗里达大学计算机系统，偷取了一些正在接受评估的新软件，特别是微软视窗95的Beta版本，那是微软创始人和世

① 米特尼克现已被假释出狱，但被严格禁止接触计算机及相关设备或从事与计算机相关行业。——译者。欲查询有关米特尼克的资料，可上网访问：www.netmarket.com.br/mitnick/，www.well.com/user/littman/game/news.html，www.2600.com/kevin/，以及alt.fan.kevin-mitnick——著者

界首富比尔·盖茨指望着用来让公司再上一个台阶的。不管怎样，今天，黑客游戏已不再困扰经济领域；虽然它对网络世界依旧是个严重威胁。黑客还可以期望再看上几回日落美景。

在追踪黑客的过程中，产生出一批新型警察——网络警察。他们承认，对他们来说，为了满足一己怪异的快感，或甚至为了犯罪目的而闯入他人系统的黑客，都比不上动手窃取软件的小偷重要。为此，1995 年新年伊始，在微软公司的坚持下，特工人员就在肯塔基州的莱克星顿破获了“BBS 刺客行会”团体。这个组织一直为诸如“采取一种姿态和拥有剃刀 1911 的海盗们”之类的黑客俱乐部藏匿黑客服务器。这次破获行动的战果给人印象相当深刻：共没收了 13 台计算机、11 台调制解调器、一个卫星天线、黑客用的 9 千兆字节数据和自 1992 年以来存档的 40 千兆字节的数字化信息。调查者在没收获得的数据中发现了视窗 95 的 Beta 版本，可以下载！

偷盗软件是桩大买卖。这些年里，规模最大的窃案当属计算机游戏窃案。小型 Atari 和 Amiga 计算机的用户往往已经发现这样做——从而把成百上千的新游戏纳入指令表——是拓展他们所喜爱的休闲活动最方便也最省钱的办法。今天，这宗交易早已大大超出少年复制团体微不足道的初衷。像任天堂等公司所创造的游戏精妙非常，使得盗版复制有厚利可图，刺激了旨在绕开原版

保护的复杂的技术手段的发展。

现在已经形成一种黑客行业，专门窃取和复制用于台式机出版、图形设计、建筑等方面最昂贵、先进的程序。这些高科技强盗首先进攻运行 Beta 版本[1] 的服务器。这种服务器同时又能够在类似网络上出售 Beta 商业版，并从售价中提取部分费用。通常，黑客得到一个软件程序后（“原供应商”特指盗取软件并在黑客圈子里加以发布的黑客），就让骇客来破解其复制保护程序。不言而喻，这种做法使正版软件业蒙受了巨大损失。据商业软件联盟的统计数字，仅法国因黑客服务器提供复制软件以及个人和公司雇员交换软件所损失的利润就达7．8亿美元。这个数字是法国计算机业因仿造所受损失总额的三分之一。

在美国，软件出版商协会（SPA）在过去几年里，对打击黑客行为越来越积极。“借”软件的观念尽管显然违法，却曾经被奉行“免费”法则的因特网世界所全盘接受。但这一点现在已发生变化。1996 年 7 月 23 日，美国出现有关的首例诉讼，软件出版商协会把“原供应商”迈克斯·巴特勒告上法庭，因为他曾经上载到文件

---

① 软件的 Beta 版指的是即将全面发行的软件的试用版本。编程员在指定用户和朋友中发表 Beta 版以便听取其试运行情况和发现问题（即网迷们常说的捉“虫”）。

传输协议（FTP）[1]。为何偏偏是巴特勒受审呢？软件出版商协会知识产权教育和实施副总裁桑德拉·塞勒斯说：这是“对那些自信能够侵犯软件版权而不必担心暴露或受惩罚的因特网用户的一次警告。虽然软件出版商协会无意监督所有因特网用户，但我们将采取强有力的措施跟踪甚器尘上的违背因特网服务商（ISP）网络操作的行为，以及对我会成员版权的侵犯行为——巴特勒先生被指控的就是这类行径。”巴特勒案因此被视为对因特网的一声警钟，钟声宣告：小心，好日子结束了。

从内部着手保护美国市场正在被赋予新的重要性。但人们应该警觉到，对知识产权最强烈的侵犯来自亚洲，特别是中国和俄罗斯。根据软件出版商协会1996年2月发布的一份声明，中俄应对无视作者权益也不付任何版税，公然违抗现行所有国际版权法规的仿制软件业的兴起负责。“实际上，仅仅一份复制的非法软件就能够满足整个国家的需要。软件出版商协会估计，1995年俄罗斯和中国使用的商业应用软件中，百分之九十以上都是非法的。紧追其后的是南朝鲜和希腊，其比例估计约为百分之八十。”在这四个国家中，授权软件制造商每年因黑客行为蒙受的损失高达7亿美元。非法软件走私正在上升到异乎寻常的比例。举个例子：1996年5

[1] FTP服务器是因特网服务商提供给订户用来下载免费软件程序的。订户也可以在FTP服务器上上载自己的软件，供其他人下载。

月在香港截住了两名黑客。他们随身携带的20张光盘，所含软件转手可卖两万美元，他们还携带了复制软件所需设备，并且早已开始把他们即将复制的软件的目录传真给各地数十家公司。

1996年5月，由于非法复制受版权保护的材料，中美关系一度趋于紧张。美国指控中国对黑客的牟利行为视而不见。据美软件出版商协会和商业软件联盟估计，1995年中国黑客获利即达4.86亿美元。按照美国政府的说法，虽然中国在1995年就和美国签署协定保证严厉打击这类活动，但到1996年春，中国广西地区有31家工厂仍然在开工制造着成百万上千万的光盘。桂林一家著名工厂每天生产两万张光盘（都是微软和其他公司程序的复制品）和音乐CD。美国对这些工厂表示关注。美国贸易代表强烈要求采取高达30亿美元的报复性制裁措施。1996年6月17日，双方达成协议，中国最终同意立即关闭15家工厂，为这一商业冲突和美国的制裁威胁划上了句号。但是，要真正了结这个问题是困难的。复制程序是如此容易和廉价，使得这个问题简直永远不可能消失。只有当保护这些软件的代码变得不可破译，许多黑客洗手不干，这个问题才可能最终解决，否则解决之日依旧是遥遥无期的明天。

放眼全球，窃取程序看来是一场巨大的经济灾难，据软件出版商协会主席肯·沃尔什计算，造成的损失每年达75亿美元。由于亚洲市场得到的软件——由中

国、印度、南朝鲜和中国台湾制造——几乎免费，实际数字要高得多。

1992年6月，德国的Cadsoft公司看厌了自家软件横遭窃取的状况，提供了一个免费的演示程序。不过，把它安装在计算机里的人们不知道，这个演示程序设计目的是搜寻出由该公司制造而又没有适当注册过的软件。这个程序发现被盗软件后，就会在屏幕上打出一个信息，邀请这些幸运的胜利者接受Cadsoft馈赠的用于该软件的免费指南。但是，如果这些人打开信箱翘首以待，他们很快就会收到来自该公司律师的一封信，要求他们赔偿6000德国马克的损失。半年之内，有400人落入这项技术设下的圈套里，其中包括德国反间谍机构联邦宪法保卫局的职员。其他软件制造商则集中精力对付可能成百上千地复制同一程序加以使用的公司。公司一旦被抓住，要受到的惩罚可远比个人用户受到的严厉。怎样处置个人侵权一直是个问题，因为既然电脑盲也能轻而易举地复制程序，绝大多数人都这样做。

迄今为止，所有与作者和版权相关的知识产权问题都是黑客行径派生出的后果。当因特网可以在几秒钟内向全球发送数量庞大的信息的时候，你如何处理版权问题？这要等某人找到办法，使得软件备份只有缴纳注册费后方能使用，那时候才会有可靠的答案。然而在相当一段时间里，这种办法是不可能找到的。

第五章 私掠船和冒险家

吉恩－伯纳德·康达特从未真正闯入过任何大型计算机系统，但他在欧洲黑客中仍然是响当当的角色。他的名声被报刊广为传扬，凡是谈论黑客行为、因特网、网络开发以及安全问题的地方，就有人谈论他。康达特靠写书、著文、开设网站以及向想要加强信息安全保护系统的公司提供服务谋生。

自称是一级专家的康达特 1963 年出生于法国的贝济耶。他节奏单调的演讲里传达出一种充满自信的孩子气的魅力。对他来说，经过这么多年的深入探索，确认自己在黑客世界的优势地位是十分重要的。显而易见，康达特从工作中得到许多乐趣，而他对法国反间谍部门——国家侦察中心的帮助也非同小可。

黑客成了警察眼线

1989 年 4 月，康达特拿到音乐研究和计算机学学位

后，来到了巴黎。此时他已经参与反间谍工作。早在1983年，康达特在法国地区电视台表演了一个朴素的、甚至不违法的黑客手段，成功地从公用电话亭连接到位于美国加利福尼亚州帕洛阿尔托的对话数据库，引起法国国家侦察中心的注意。后者把康达特招至麾下，让他到处去以黑客手段刺探会议情报。康达特甚至在欺骗其他黑客时也散发着魅力，引起人们注意。他说："我采纳一个家伙告诉我的做法，让另一个家伙相信是我做过的……"

1989年年底，康达特的上司让一鲁克·德拉考决定让这匹年轻的小马驹首次执行重大任务。在法国国家侦察中心总部附近涅拉滕街的一家酒吧里，康达特接受了任务。80年代初期，传言说汉堡的混沌计算机俱乐部可能和克格勃有关，人们很想知道是否还牵涉到法国公司。法国国家侦察中心于是策划了法国混沌计算机俱乐部，由康达特任主席。到1990年初，康达特施展浑身解数，把许多年轻黑客都吸引到这个俱乐部中来，警方因而对他们的情况了如指掌，能够在必要的时候抓住他们。

这项工作说来轻巧，做也不难。康达特擅长不引人注意地四处刺探情报，渐渐以白狼知名。那些最轻信的人觉得法国混沌计算机俱乐部是个神话，多疑的人则疑心它是警方一个据点。

法国混沌计算机俱乐部很快就开始引起黑客和媒体

的注意。但最主要的是，它向警方透露了谁在操办复制软件的盛宴，谁又在干其他违法的事情。一位可靠的法国国家侦察中心人士肯定地说："康达特就好像通往海盗世界的一座小桥，但他从来不代表我们搞任何黑客行为，我们对他的利用是防御性的，是为了保护自己的利益，从来不拿他当进攻性武器使。但是，比如说，有人闯进汤姆森或 Pehiney 公司的时候，他帮我们重构他们的网络。这对他并不很难，事实如此，牛皮也是有限度的。"

康达特舒适地"沐浴"在法国国家侦察中心的"聚光灯"下。无论什么时候他去电话，国家侦察中心就会立马派出视察员来监督一回有趣的谈话，或者是更新某人的档案材料。无论他什么时候离开巴黎，国家侦察中心都派人跟随。倒不是怕他飞了——他干吗要飞呢？而是不想让其他警方机构接触他。

法国国家侦察中心把事情搞成了一场杂耍。它印制了几百件 T 恤衫，让康达特发给他的追随者，又印了几千张印有康达特面孔的明信片。1991 年 9 月 17 日，康达特出席了一个电视谈话节目，我和另外几个人也应邀参加，话题是间谍活动对普通公民生活的影响。节目主持人、记者丹尼尔·毕拉连告诉观众，警察就在房间里面，目的是保证康达特的演讲不会泄露过深的隐秘。在节目中，康达特通过耳机从他在国家侦察中心的顶头上司那里了解谈话情况。这位"黑客"叙述了他曾经如何

进入 TGV 公司计算机，预订了巴黎至里昂间高速火车的全部座位。事实是，确曾另外有人潜入过 TGV 公司的计算机系统，但这无关紧要。

闯入 TGV 公司计算机的黑客中，有一位最近对我谈起了康达特，说他曾经“非常能干和有勇气，但不是特别谨慎。”黑客和经常出入黑客圈子的人们看来都有相同的冲动，渴望把一切公之于众。如果不能自吹自擂一番，那黑客生涯就的确枯燥乏味了。而且如果康达特“真的后悔”把那么多友善的年轻黑客出卖给国家侦察中心，他可以肯定许多年轻黑客也在玩相同的游戏：“人人都高谈阔论，但到我这儿付出了重大代价。人们来看我，我就写出关于他们的详尽报告交给国家侦察中心。两天以后，那帮反间谍特工就会在早上六点钟敲他们的门。我本不应该这么做，我现在本该娶妻生子，有房有车，而不是像条狗那样四处流浪，抬不起头……”

康达特说，这些游戏都结束了。1991 年，警察头子丹尼尔·帕杜安（现主管信息技术诈骗调查局）为一起电话黑客事件逮捕了他。康达特后来被无罪释放，但他至今相信自己更大程度上是不同警察部门进行黑客竞争的牺牲品，而且郁郁寡欢，觉得国家侦察中心纯粹就是抛弃了他，听凭他自己去竭力摆脱那些没有根据的指控。

在谍报机构历史上，到处可见那些被榨干利用价值后遭到抛弃的可怜虫。但康达特却还是一个能干的、知

识渊博的年青人。他经常被邀请当顾问，甚至在涉及黑客的案子里充当专业证人。他为许多家报纸撰稿，也经常在欧洲电视节目和法国计算机服务网上论坛上露面。1997年伊始，他还当上了德国一家国内电子安全公司驻法办事处的头头。往事是否真的会永远伴随着康达特，这还得走着瞧。

黑客的地狱

黑客玩的是猫和老鼠的小把戏，很少捞到大猎物。这种可能性之所以十分有限，是因为一旦他们掌握了能干成大事的专业技术，他们的臭名声也就高到自我暴露的地步。前面说过，有些失败更多是由于他人的背叛，因为黑客世界已经完全被康达特之流的做法破坏得四分五裂了。不管黑客们是否愿意相信，自由穿梭于网络空间的黑客非常罕见。所有讨论黑客主题的新闻组，所有黑客的服务器，无一例外都受到各国警察不舍昼夜地监视。

黑客往往有多热情，就有多天真，他们总是想不到他们的所作所为会带来的各种人事和法律后果。黑客的想象力奔放不羁，多年以前，就和他们围攻的对象（这些人往往依旧对系统所受威胁漠不关心）发生了第一次冲突。从那时起，他们就受到司法系统的追捕。一些聪明的年轻黑客很快就明白这些恶作剧会让他们付出什么

样的代价。1988年，法国通过高弗温法[①]，以法律手段坚决阻止黑客进入重要计算机系统。

80年代初，法国黑客曾有过一段辉煌的日子，此后成就便显得十分有限，原因是他们天真的恶作剧很快就发出了馊味。法国国外安全总局，特别是国家侦察中心，过去都是诱使间谍叛变的艺术大师。它们充分利用了这些方面所有屡试不爽的技巧，康达特的遭遇就表明了这一点。从来没有哪个机构会对此予以公开承认，但紧闭的门背后，人们的嘴并没有被封死。假如“受害者”不那么急于倾诉的话，理由就和谍报以及双重间谍的历史一样古老。

从人口统计学上讲，黑客总体上属于一个排他性群体，他们是年轻的受过良好教育的计算机学系学生，用业余时间攀登防火墙。出没地点则众所周知——几所特殊工程学校和信息安全企业。当受害者察觉遭到侵入时（一般都会知道），最终抓不到黑客的情况越来越罕见。查获大量被盗信息或者逮捕某个康达特之流的人物通常都有助于让人们的神经暂时平静下来。

把手伸入虚拟的饼干筒的年轻黑客，往往一被捕就

---

① 高弗温法规定：远程计算机闯入应判处一年以下监禁和一万美元以下罚款；如果在这个过程中计算机遭到损坏，或者数据被毁，则刑期可增至三年以下，罚款10万美元以下；如果被窃数据用于非法目的，则刑期可增至最高五年、罚款40万美元以下。高弗温法全文见于网址：www.cicrp.jussieu.fr/cicrp/loi-info.html

发现自己抓着了放不下手的烫山芋。有时警察让司法部门接手处理，黑客就得上法庭，而且所有的麻烦都像是在说：法官对黑客严厉无情。有时，警察就象对待被当场逮住的间谍一样，询问黑客是否愿意金盆洗手，同警方合作。光密告几个朋友可不够，还必须签约为谍报机构工作。在过去几年里，没有几位黑客能够拒绝这种“邀请”，特别是被抓住时年龄在 21 岁左右的黑客。21 岁是法国男子应征入伍的年龄。

黑客变节，改为警察效劳，那时辰可谓是噩梦成真。不管这个黑客多么擅长以自己的方式截取计算机通讯（口令、密码等等），如果碰到传统调查手段更易得手的信息，例如根据用户个人情况而变化的口令——生日、宠物姓名、写在显示器旁边一张纸上的一段话等等，他们就远不如警察了。警察特殊的情报搜集技巧，再加上黑客破译密码软件能力，能够产生出丰硕的合作成果。

对黑客来说，这是一桩交易，既不好玩也非游戏。他们偷偷进入银行计算机浏览犯罪嫌疑人的帐户，试图制造事端，或者甚至取走存款。他们闯入个人计算机的密门（至少是带有调制解调器的个人计算机）。而且，即便对方没有调制解调器，也不要紧。黑客自有办法巴结他们想通过调制解调器连接的计算机用户。许多轻信的受害者都是从邮件中收到免费的调制解调器后，不假思索地就加以连接和使用。

黑客随即就使用“嗅探”程序来截取用户的登录号（上网密码），并在遇到授权用户的风险较小的时候回拨，但有时候可没这么容易。现在有种技术能够帮助伪装计算机身份代码，包括可以在网上找到的电子复邮器，它能够通过一系列连续的节点转换来隐藏发件人的地址。1994年以来投入使用的匿名服务器（多谢芬兰的约翰·赫尔辛吉乌斯）还可以保护和服务器相连的计算机的真实身份。事实上，匿名的芬兰服务器不会永远流行。1996年8月30日，赫尔辛吉乌斯宣布他正在结束这项服务，芬兰政府确认了这个消息，声称基督教科学论派已提出起诉，并断言赫尔辛吉乌斯的行为违反了芬兰法律[①]。赫尔辛吉乌斯向网民解释了自己的决定。他说：“我暂时关闭复邮器是因为在芬兰，管理整个因特网的法律问题还没有得到界定，对用户的合法保护尚需澄清。眼下，因特网信息的隐私问题在法理上还不明朗……这些复邮器使人们得以在网上匿名和秘密地讨论一些非常敏感的问题，例如家庭暴力、校园暴力以及人权问题等等。对他们来说，复邮器的关闭是个严重的问题。”在复邮器关闭的前几天，英国《观察家》报发表

① 赫尔辛吉乌斯的电子邮件地址：anon@penet.fi 匿名服务器的保护是一种假象。1995年，允许黑客发送从基督教科学论派偷来的文件的芬兰服务器向警察报告了用户的身份。欲了解匿名服务器或赫尔辛吉乌斯事件的更多情况，可访问新闻组：alt.anon 或网址：www.stack.nl/galactus/remailers/index - penet.html

文章猛烈抨击了赫尔辛吉乌斯—— 这和他的决定没什么关系。文章大量引用未经证实的说法，指控赫尔辛吉乌斯允许其服务器传输儿童色情资料。事实是，就连芬兰警方后来也承认，赫尔辛吉乌斯在1995年就采取预防措施，从技术上杜绝了传输儿童色情资料的可能。今天，无论谁都不能保证一定能够发现攻击源，就连谍报机构也逐渐认识到这一点。其结果不足为奇：绝大多数国家驻外使馆的计算机系统都远离网络——远离所有网络。否则他们就太冒险了。

艾米斯风暴

前面讲过阿尔德里奇·艾米斯的被捕情况。他简直就是直接从间谍小说中走出的坏蛋。艾米斯为美国中央情报局工作多年，负责处理美国（有时是英国）特工挖出的苏联间谍。他以无限的热情和惊人的规律性从事着背叛中情局的活动，直到1993年才暴露。当时，联邦调查局想在逮捕之前搞清楚艾米斯的全部活动能量。高级调查员莱斯利·G·威舍领导的小组受命就此立案调查。威舍的小组立刻想方设法要闯入艾米斯家中的个人计算机。不幸的是（至少对联邦调查局来说），艾米斯没有上网，他的计算机甚至没有调制解调器。他还在用手敲出给克格勃上司的情报，然后把它们丢弃在华盛顿的废纸篓里。这件事表明，防范入侵的最佳措施仍然是

不上网，虽然如今随着因特网的普及，这个做法实际上越来越不现实。由于艾米斯的计算机不连任何东西，联邦调查局调查员决定利用一项鲜为人知的技术，通过无线电接收器截取艾米斯计算机发出的电磁脉冲。

凡在家中或办公室使用个人计算机并想保守信息秘密的人应该知道，他们的计算机实际上就是无线电传输器。键盘、中央处理单元（CPU）、连接电线、显示器，以及打印机全都构成电磁辐射源，专家们把这些发射称为“泄露性寄生信号”或“红色信号”，诸如“动力科学 A－110b”（1kHZ－1GHZ）之类的某些尖端无线电接收器能够轻而易举地识别出它们。从 60 年代初期起，这些电磁波就广为人知，受到大规模研究。在国家安全局的倡导和技术指导下，“风暴”（Tempest）现已成为反侵入技术的规范。“风暴”十分隐秘，就连提出“风暴”系统和这个名字的工程师都不准说出它的首字母缩写词。它表示的概念很多，最含混的两个看来是“防范虚假传输辐射的完全电子和机械保护”技术，以及“终止电磁脉冲环境安保技术”。

阿尔德里奇·艾米斯差点就正式成为这项技术的第一位牺牲品。据信，这些红色信号有时能够发射几百码。在艾米斯一案中，联邦调查局经测试发现信号不能超出艾米斯和妻子罗萨里奥的住宅 82 码之外。这套住宅价值 50 万美金，以现金支付（而且没有引起中情局警觉）。它坐落在华盛顿特区一个幽静的居民区里，假

如附近停上一辆监视车，像艾米斯这样的职业特工立刻就会注意到。所以联邦调查局认为最好还是让艾米斯出几天远门。

干谍报这一行，搜查可谓家常便饭，而且已被修炼成一门艺术。特工们事先细致地勘察地点，然后运用高超的技术手段悄然潜入，离开时能够不留任何蛛丝马迹，察觉他们的光临几乎是不可能的事。在艾米斯豪宅里，特工们不仅安装了几十个扩音器，而且还复制了他的计算机硬盘。一位专家在彻底检查硬盘之后，发现了艾米斯和俄罗斯之间的通讯联络，那是艾米斯以为早就删除了的。

面对最近突然出现的逮捕风暴，人们会疑惑地想，究竟美国情报界还藏有多少鼹鼠呢？遗憾的是，既然这类犯罪活动的首要动机是贪婪，将来就大有可能再发现新的鼹鼠。以 1996 年 11 月被捕的哈罗德·J·尼科尔森为例。80 年代初期，尼科尔森曾是中情局布加勒斯特分部负责人，后被调往吉隆坡。1994 年，他开始为俄罗斯搜集情报。他在离弗吉尼亚州威廉斯堡不远的皮里地营负责训练中情局新雇员，把全部学生名字都交给了他的俄罗斯联络人，后者为此举手之劳付给尼科尔森优厚的报酬。不仅如此，尼科尔森还利用他清白无瑕的安全记录，接触到中情局计算机里的机密级文件，并把它们送给了俄国人。1997 年 3 月 3 日在弗吉尼亚亚历山德拉联邦法庭，他认罪服法，得以免判终身监禁，尽管结

局也好不了太多。三天后，前联邦调查局特工伊尔·皮梯斯也低头认罪。皮梯斯从1984年起就为俄国人搜集情报，不过他所接触到的情报远没有那么敏感。

许多间谍都是因为个人计算机遭到偷袭而落入法网的。虽然有的软件能在计算机遭到入侵时向用户发出警告（还有软件能阻止侵入者进行复制），但阿尔德里奇·艾米斯当时完全没有采取防范措施。一位专家肯定地说，进入艾米斯的计算机时，联邦调查局毫不费力地在里面安装了一个实时无线电传输器（无疑是和键盘电路相连），特工们因而可以在适当距离外收到非常清晰的信号。

几个月后，艾米斯被解职。1994年4月，他对自己的罪行供认不讳，但和当局约定不公开进行审判，妻子免受起诉。艾米斯的罪名涉及他为苏联进行的谍报活动和逃税——没有申报他从克格勃那里得到的460万美元报酬。除去为妻子罗萨里奥在哥伦比亚购置的地产之外(罗萨里奥来自哥伦比亚，在墨西哥哥伦比亚大使馆工作时和奉中情局之命前往墨西哥公干的艾米斯相遇)，他用克格勃的钱买的所有东西都被没收。他本人注定要在监狱度过余生，无假释机会。

法国式风暴

80年代后期，法国国防部某些高级官员迎来了一

批不速之客。军队技术人员和网络安全专家满心欢喜、步履轻快地走进了各位政府要人的办公室，建议他们到停在下面街上的卡车里溜上一眼。在卡车里，这些大人物看见屏幕上显示出的竟是他们的办公室。他们的秘书正在里面工作。所有这些都被截取和再现在远程计算机屏幕上，而且他们，或者任何人，都能听见秘书们敲打键盘的声音从一片虚空中传来。最近，电子武器中心向我和其他几位记者展示了这些技术，他们开始广泛采取措施，以期让军方计算机用户醒悟到，他们的轻率从事容易招致外来侵犯。

法国没有法律禁止截取计算机无线电波。绝大多数用户，不论私营还是公共部门，抑或是产业部门，也都丝毫没有警觉到他们的隐私处于危险之中。这使得谍报机构能够轻松自如地浏览个人用户的计算机信息，就像那是桌面上摊开的一本书一样。

在特定条件下，使用膝上型电脑能够限制信息的读取，因为它们散发的辐射较一般台式机要少。有时，专门截取信息的奥威尔式窃听者会茫然不知所措，因为无法从一间有 100 台电脑的房间里提取个别电脑发出的辐射：要识别它们几乎是不可能的。

在很大程度上，“风暴”技术也是依靠把一定水准的加密术限制为政府专用，以便谍报机构轻易查看普通公民的文件。平头百姓甚至企业不经特别许可都接触不到这项技术。这自然对力图维护计算机安全的当局提供

了最大保护，而且也保证他们能够继续截取他人计算机发出的辐射。

美国于1974年开始使用“风暴”系统。受这一系统保护的个人计算机是个碉堡式的工作台。其基本原理是把系统中可暴露其存在的任何部件都变成一个微型的法拉第笼，即处于封闭状态，防止无线电波外泄。“风暴”技术所保护的主体计算机看上去就像坦克一样，有大量被屏蔽的电线和笨重庞大的受特殊安全防护的插座。唯独计算机屏幕显然一如既往地没有变化，保护它的是一个几乎看不见的细小的格栅。在美国，制造“风暴”硬件零部件的公司有50多家，按照“风暴”设计者所要求的高标准来生产这些零部件，所需费用是设备成本的两倍。

不过，对最具敏感性的外交设施来说，钱不是问题。安装“风暴”计算机的整个房间都按法拉第笼原则设计，透不出一丝辐射。人们不可能比这更小心了，因为“笼子”即便开了最细微的一条缝，无线电波也能像群麻雀一样飞出去。使用“风暴”设施的用户讲述了一个负责看守这类法拉第笼的守夜人的故事。在一次例行辐射检查时，技术人员发现尽管采取了所有安保和特殊措施，无线电波还是在源源不断地外泄。技术人员苦恼了几分钟，但迅速找到了症结所在：蠢得讨厌的守夜人在墙上钻了个洞，以便把一根电视天线拉入房间，因为他的天线在这个法拉第笼里什么信号都收不到（这正是

设计的目的!)。这个洞被迅速堵住，法拉第笼又固若金汤了。

只能在网上看到的第一本网络小说《停止妥协》[1]就是以“风暴”规范为基础写成的。该书作者温·施瓦陶是美国最高级的计算机安全专家之一。小说描绘了一个颇具煽动性的情景：日本为了报复美国在二战中取得的胜利，侵入了美国的计算机系统。新的经济情报领袖罗伯特·D·斯蒂勒经营的“开放源解决办法”公司正在急于插足世界经济的重要部门，他相信忽略“风暴”的重要性将会造成巨大损失：“绝大多数美国公司没有充分认识到，外界有多么容易打进他们的机构；而且绝大多数公司也不进行重要的工业谍报活动。例如，绝大多数美国公司绝对缺乏计算机安全，也不采取措施保护其计算机免受外部侵入。他们完全没有意识到，他们的计算机屏幕和计算机辐射很容易就被停在他们建筑物外面的货车所截获，美国公司普遍觉得工业谍报‘不值得’。”

英国电讯遭袭击

谍报机构也会遭到黑客袭击。近年来，最不寻常的一次攻击发生在 1994 年的英国。一名设法进入英国电

---

① 此书可在施瓦陶个人主页：www.infowar.com 上看到。

讯（英国主要的电话公司）计算机的黑客竟能找出该公司最机密的资料——包括当时英国首相约翰·梅杰在内的所有政府成员家庭电话号码名单，以及英国谍报机构——MI6（国外谍报）、MI5（国内谍报）和负责安全问题的政府通讯总部——的所有负责人的电话号码。

记者斯蒂芬·弗莱明在《独立报》上披露了这一事件，引起巨大骚动。黑客是通过因特网，从一个匿名服务器将这些超级机密资料传给弗莱明的。这位黑客解释说，他在发现英国电讯公司的大型中央计算机里有几个“有趣的”弱点之后，曾经设法到英国电讯公司应聘当临时雇员。他甚至发现了闪烁在公司职员各人计算机屏幕上的秘密代码，得以随意访问最罕见登记的英国电话号码名单：这些职员听任他们的密码在屏幕上闪烁，以致趁他们度假时临时代职的雇员不费吹灰之力就接触到受超级保护的中央系统。这种灾难性的、愚蠢的人为错误可彻底破坏所有高科技防火墙和反黑客软件。显然，防范愚蠢的人为失误是超出人们意料的更大的挑战。

第六章 网络警察的黄金时代

大多数部门——军队、大企业、教育乃至武装力量——都严重地依赖着计算机。尽管社会没有计算机也能运作，但从超市条码阅读器到高速公路的收费亭，从文字处理到飞机起降，计算机现在在我们日常生活中发挥着强有力的作用，对此无人能予以否认。各个公司都在自行建立网络，以便雇员相互交流；越来越多的“游牧民”走出办公室，通过上网和同事联系；而他们所认识的同事，只不过是脱离肉体的游荡着的声音和一束又一束比特。

利害攸关的信息安全世界

这些系统的依赖性和整合性是至关重要的。重大的计算机错误能够使一个公司甚而一个国家瘫痪。举个例子，记者就很清楚最小的计算机故障也能让编辑室变成狼藉不堪的混战场。而且，他们担忧的不只是黑客。专

业技术人员在对付黑客方面已经取得了很大进展，他们现在正奋斗在其他阵线上。因为除却黑客侵入，酿成灾难的手段还有很多种，如火灾、软件故障等等。卡内基-梅隆大学的计算机紧急反应小组仍是欧洲各地群起效仿的样板。法国国家标准和技术研究所的国家计算机系统实验室则推出事故处理和安全小组模式，这是一个成员遍及全国的专家网，他们通过因特网可以对各种紧急情况立即作出反应。公司内部心怀鬼胎的操作员能够造成山崩一般巨大的突发性灾难（通常是经济方面的），人们对这方面的计算机犯罪进行了详尽的研究[①]。

在欧洲，法国成立了综合性计算机安全组织，名叫法国信息安全俱乐部（CLUSIF），这是法国保险公司全体大会（APSAD）的一个分支。在一份 1986 年至 1990 年的评估报告中，法国信息安全俱乐部指出，最严重的计算机灾难都和盗用公款以及虚拟破坏有关。内部黑客或“叛徒”搞起破坏来其创造性一点不比黑客差，区别不过是玩的把戏大小。犯罪者使用简单巧妙的技术，顷刻之间就能捞到成千上万美元，那些充分利用全球银行系统计算机化的人当真能一夜暴富。有个“叛徒”曾在瑞士苏黎世一家银行设法假转帐 1600 万美元。与此同时，他发出一张假订单，从莫斯科求购同等价值的钻

① 利物浦大学白领犯罪研究部发现，绝大多数盗用或挪用公款罪行都是白领所为。参见网址：http：//www.indigo-net.com/lmr.html

石。这一切都是在同一家银行进行的。瑞士银行垫付了钻石款并将钻石送交客户，但作为整个交易的基础的所谓美国巨款却一直没有到达目的地。某某人只要在另一家银行伪造一个现行汇率入口，立刻就赚了 1500 万美元。

黑客在法国信息安全俱乐部的报告中也占有一席之地，虽然这份报告连黑客所攻击的公司名字都闹错了。德国混沌计算机俱乐部袭击了一家储蓄银行的电话交换台，馈通 1．3 万个电话，花了这家银行 8 万美元。同一时期，另一家银行为了使系统摆脱掉一个简单的病毒，付出了十倍于此的代价。不过，它们还都不是这方面的世界纪录。几位邪恶的黑客摧毁了一家银行的安全系统和所有帐户记录，这家银行——不说名字了——为此损失 2000 万美元！

有些情形下，调查者找不出犯罪作恶者。但计算机专业人员，还有谍报机构和新生的网络警察，一直在寻找更好的方式加强所有各种系统的安全（对此，新一代黑客在为联邦调查局工作之前，还不得不想法子绕过去）。在这个过渡时期，法国信息安全俱乐部努力让各公司认识到：衡量他们生存状况的标准，取决于他们保护计算机信息的自觉性和能力高低。法国信息安全俱乐部秘书长让-马克·阿卢埃特说："即便是家里的计算机系统，其内容的价值也几乎十倍于机器本身的价值。"这一断言无疑会让大多数计算机用户感到惊奇。

甚至妄想狂也有敌人

很明显，就像鼓吹因特网的人喜欢说的那样，因特网带来了自由。尽管如此，谍报机构显然一直在把这些自由工具转变成进行社会监控的新手段。而且，随着因特网作为战争武器其军事用途的大量增加，因特网实际的自由度也越来越恍如镜花水月；即时通讯不可否认的好处和随之而来的弊端——政府进一步侵犯公民私生活——之间越来越难以划清界线。早在 1977 年，美国隐私保护研究委员会就注意到："真正的危险在于：由于对众多小型、单独的记录储存系统进行自动控制、综合集成以及互相连接，个人自由逐渐受到了侵蚀。虽然孤立地看，这些系统可能都是无害的，甚至是有益的，而且完全是正当的。[①]"尽管立法者试图抵挡这不可抗拒的潮流，显而易见，这一幻象已经成为现实[②]。

当然，1948 年乔治·奥威尔在写作《一九八四》一书时，就已经预见到这所有的一切。他杜撰的一个无所不在的窥视公民生活的政府探子——"老大哥"，如今就生活在我们中间。忽视他的存在就跟认定我们无力防

① 参见网址：http：//cpsr.org/cpsr/factshts

② 1986年 6 月，国会通过电子通讯隐私法。参见网址：http：//www.pls.com：8001/his/12.html

范“老大哥”用来窥视公共和私下场合的电子眼一样，是种短视行为。

在计算机安全研究所工作的约翰·奥利瑞承认：“捍卫公民自由的人在隐私问题上歇斯底里地大喊大叫，但他们的论调是不切实际的。”克劳德－玛丽·瓦多特和路易塞特·古韦尔内合写过一本有关现代社会控制手段的著作，在法国备受重视。他们相信，现代社会碰到了一种“计算机极权主义”；“政府和私营部门里有群高水平的程序员正在成功地发动一场技术政变，并得到着眼于安全和检验市场的制造商们的全力支持。”这可能说得太过分了。

不管怎样，自命为现实主义者的人们争辩说，不可能指望谍报机构同时监听成百上千个电话，更不用说扫描像因特网这么浩瀚的网络。他们忽视了超文本之类的分析工具和人工智能领域所取得的巨大进展。从1994年起，美国国际商用机器公司就设计出一种供个人计算机用户使用的系统，它像虚拟速记员一样，能够即时听写，把口授指令立即变成文字内容。最没有想象力的人也能看出，这样一种工具落到谍报机构手里，就可以被用来把电话通讯自动转录成数字文本。下一章中我们将会看到，类似“泰加”（Taiga）和“主题”（Topic）这样的分析“引擎”能够即时编写文件摘要，将关键字词和概念突出出来。

当然，世界上绝大多数警察机构都还没有这般先

进，至少目前还没有。只有美国国家安全局、英国政府通讯总部、法国国外安全总局、德国联邦情报局，以及俄罗斯对外情报局拥有这种先进手段。他们大多数活动依然十分隐秘，以至于简直不可能确定他们目前的技术水准，后者完全取决于他们武器库里有多大的数字捣弄能力。

你能算"安全狂"吗？

任何人只要仔细看看每个月的电话清单，就明白我们的隐私受到多大威胁。电话清单告诉我们些什么呢？我们拨打的电话号码、打电话的日期、还有我们每次通话用掉的时间。陌生人从这些信息里可以清楚地了解到我们与人交往的情形。迄今为止，人们无法阻止这种信息被编译，也几乎没有办法防止那些觊觎我们公司的人利用这些信息。

在商界，公司电讯的负责人可以识别出哪个雇员打电话，哪个雇员接过电话，然后利用现代统计分析方法（PABX，即专用自动分支交换）来分解这些电话。他们能够测定向某个国家打出电话的频繁程度以及是否与生意有关。没有什么能阻止管理人员搜集这些情况。

公司给你免费的因特网访问权限吗？这其中利害参半。你的上司会对哪种服务器被拨叫了如指掌。如果它们与公司业务有关，万事大吉；如果雇员上网是在玩交

互式游戏或者下载不堪入目的色情照片，老板肯定能发现。通常情况下，老板要抓的是大鱼，不去理会属下的小把戏。但一旦发生劳资纠纷，不必惊讶，这类把柄就会突然派上用场了。假如这类集体监视看上去有点不可思议，再想一想。一天 24 小时监督计算机运行的公司比比皆是。它们不只是观察雇员上下班时间，而且还监督他们的工作情况。程序员赋予管理人员直接从任一雇员的工作站馈收信号的能力，他们因而可以看到雇员计算机屏上正在显示的内容。

任何人都免不了受到这类侵犯，甚至记者也不例外。在巴黎，对某些记者来说，计算机屏幕突然失灵几分钟是常事，没有理由恐慌，这只是报纸编辑通过记者计算机屏"镜子"，在检查记者工作的进展情况。费拉隆（Farallon）制造的"廷巴克图"（Timbuktu）程序在这方面的应用上表现出色，可使主管人员远程遥控载有同一程序的计算机。只要对所有电话和调制解调器进行适当设置，身在纽约的主管人员就能够观察到远在洛杉矶的雇员的工作进程，这使得"廷巴克图"程序成为无可挑剔的超公司侦察工具。市场上其他程序，诸如诺顿·兰伯特开发的 Close - up/LAN、动力公司生产的 Peak & Spy、微机公司（Microcom）的 LANlord 以及 Neon 软件公司的 NetMinder，包装上全都写着它们是"改善组织"和"提高生产力"的手段，但实际上，"……它们把雇员的小天地变成了隐蔽的窃听站。还有一些应用软件可

测算出每分钟键盘敲击的次数，雇员的出错率，完成每项工作所耗费的时间，以及离机时间。不足为奇，这类技术潜在的极权倾向令隐私卫士和普通上班族都多少患有点妄想狂症状。”

监督工作场所的生产效率还不是最后目的。雇主还可以通过其他系统，追踪雇员动向，从而在任何时候都对雇员所处位置一清二楚。利用现代监控工具，雇主还可以确保只有持证雇员进入工作场所，他们的朋友、家人，或者犯罪分子都无从潜入。磁卡出入证不够，指纹检验也不够，生物力学已经越来越尖端复杂：我们的耳廓、视网膜和声音都要和安全计算机内储存的“原始档案”进行查校比对，从而立即全面地核对身份。如果这不够令人毛骨悚然，更可怕的还在后面……

零库存和追踪

在网络逻辑如何改变商业运作方面，最好的例子之一当推交通：火车、长短途卡车运输，以及公交车辆全都受到网络影响。通宵航运公司，如联邦捷运公司、联合包裹运输公司以及敦豪国际航空快件有限公司（DHL）的经营方式都因这一新技术而发生深刻的变化。大多数司机持有移动电话，一些货车配备了卫星天线，就算司机不大情愿，也能够准确地向老板报告车辆所在方位。军事运输也用上了类似的卫星技术。军用卡车往

往装备有小型天线，通过卫星中继将它们的方位传回给地面。

全世界的科学技术都在突飞猛进地发展。零库存和追踪正在取代陈旧的仓储概念。这两个系统都确保公司再也不必储存几百种乃至上千种当时不需要的货物，而是需要的时候再购买，从而节省了巨额库存费用。计算机化跟踪技术使公司可以通过计算机立即订购货物，紧接着，某个通宵递送服务公司（能够跟踪每一包裹的全部收发过程）就会把货物送达用户手中，立刻得到满意的反馈！

长期以来，军队一直利用 DECCA 或 Locan C 等系统，通过电波探测器或雷达来追踪车辆移动。五角大楼还推出了一种名叫 GPS Navstar 的新系统，这是一个 24 小时与地球的相对位置不变的卫星网络，能够跟踪单个士兵的移动，误差在离他们确切位置几英尺之内（观众从电影《爱国者游戏》里可以看到这个系统的实物大模型）。人们能够通过跟袖珍计算器差不多大的手提装置来接收 GPS（全球定位系统）数据，而不必依靠复杂巧妙的机器组合和技术人员来进行信息处理。它们甚至还能被安装在导弹的导航系统里。游艇驾驶员、徒步旅行者，以及船运公司老板，都可以花上几百美元买到精确度较差的同类技术设备（精确度为 100 到 1000 英尺）。营销这类商用跟踪系统的公司所提供的设备足以让你挑得眼花缭乱，其中包括集成便携式计算机、光码阅读器和 GPS 接收器，

它们都可以和公司总部实时链接。

要赶上零库存之类新型仓储方式的发展，跟踪技术就不得不高科技化。1995年1月的《在线》杂志发表过一篇引人注目的文章，描述了卡车司机沃尔特·马古埃尔的新生活：美国施奈德国民公司在马古埃尔的司机室安装了一台计算机，马古埃尔对它是“一见生憎”，而且对这位朝夕相处的搭档只有越来越讨厌。这台计算机通过卫星和OmniTRACS网络相连，以后者为中继，将车辆情况，如速度、每分钟转速、汽油里数和精确到100英尺以内的方位，全都反馈给施奈德国民公司和其他汽车运输公司。对马古埃尔这样的司机来说，这是一场噩梦：他们当初选择卡车生涯，原本为的是开放路面的自由。

计算机和自由

人类社会行为专业的学生有朝一日应当实地比较一下不同国家对待“机密信息”问题的态度。在美国，要弄到私人公司财务状况方面的资料几乎是不可能的；而在法国，许多数据库里都能找到这些东西。另一方面，在美国，很容易发现有关驾驶记录、个人病历以及信用度之类的材料；而在法国，这类个人资料由医疗机构和政府监督组织慎重保管，法律禁止它们向任何人透露这些信息。当然，如果有人坚决想弄到，那也总有法子。

为了得到犯罪嫌疑人的有用情况，欧洲各国警方一直都在破坏彼此的合作伙伴关系。尽管困难重重，失望多多，但坚持就是胜利，欧洲警方现在终于建立起一个实用的运作体制（命名为 C—SIS，即 Schengen 信息系统），可以共享泛欧数据库中的资料。不过，并非所有人都为此而欢欣鼓舞。

有两位专家抱怨说："我们陷入了蜘蛛网中，一种缩微的"老大哥"模式。在这张网里，我们的一举一动都被汇编成计算机信息。虽然搜集这些情报并无极权主义意图，但历史清楚地表明，鉴于未来变幻莫测，民主社会不应当允许搜集这些关键时刻可用来侵害公民利益的敏感的个人资料。"全法信息自由委员会的每份报告都正是从这一角度出发，详尽叙述了主张任人接触档案的人士针对该组织挑起的一系列小型法律纠纷。在最近一份报告中，全法信息自由委员会披露了法国西南部警察前不久创建的"MUGA—恐怖主义"档案（恐怖主义者档案联合管理系统）。法国西南部有大量巴斯克人聚居，这份文件标出了各种特别有可能发生在该地区的恐怖主义活动。

伊斯兰一瞥

利用因特网互通声气的团体，往往受到谍报机构的密切监视。在整个网络空间，有很多这类由伊斯兰原教

旨主义者组成的团体。在阿尔及利亚制造多起血腥事件的伊斯兰武装组织就通过圣迭戈的美国伊斯兰组织在网上自吹自擂。种种事实表明，在美国，因特网正在成为伊斯兰组织招募信徒的卓有成效的工具，特别是在大学里。1994年夏天，一位住在纽约的阿尔及利亚人报告说："在布鲁克林的工艺研究所，20名北非教授中就有15名对伊斯兰阵线抱热烈的同情态度。"

不难理解，对好战分子来说，因特网的魅力在于即时性全球多向通讯。像阿尔及利亚裔美国人全国协会（AANA）或者北美伊斯兰教大会（IANA）之类的合法组织往往不知不觉间就会被好战分子当作阵地。后者利用邮件列表来传播他们的观点。

在美国各大学，穆斯林学生创建了专门讨论伊斯兰教的网络。这些网络经常受到管理员的密切监督，但校方明智地选择了不干涉政策。在俄亥俄州立大学，穆斯林学生在所有伊斯兰因特网中心都发布了他们的时事通讯——"MSA新闻"（通常每天20篇新文章），并设置了一个"世界伊斯兰资源向导"，给出29个国家的200多个可供进一步查询的信息源（有虚拟的，也有实际存在的）。谍报机构使用假身份订购了所有这些时事通讯，企图挖掘到和武装活动及好战主张有关的内部消息。但是，顺着因特网回溯信息源并不总是那么容易。专家们对如何隐藏甚至假造电子地址知道得一清二楚。这类诡计要想成功，就必须在尤尼克斯网络上操作，而这个操

作系统只有威力奇大的计算机上才有。警方还慎密地研究 USENET 网上的新闻组，了解有关主题的讨论情况，以期发现潜藏的新"主顾"。在为写作此书而进行的调研过程中，我偶然听到一个我无从证实的情况：伊斯兰好战分子是从法国国防部的心脏连上因特网的。

民兵和新纳粹

看来，网络警察密切注视着网上的穆斯林，但并不为新纳粹而苦恼。但这些煽动仇恨的人非常活跃，并且受到了监督反犹言论和其他挑衅观点的网络"数字突击队"的追捕。网上有不计其数的类似"alt.revisionism"这样的新闻组，其中聊天者的观点都十分相似。但有些看似不大可能的地方，比如在讨论一战、二战以及 20 世纪历史的新闻组，人们也能发现类似的情绪流露。讨论拜物主义的新闻组也可能会谈到纳粹制服的象征意义，而讨论"纯"意识形态的新闻组很快就会转移话题，喋喋不休地说起巫术和魔鬼崇拜。

对付这些间歇发作的仇恨浪潮，最常见的反应是绝不宽容。网络社会的领导者亲自控制着事态发展。要干扰在线仇恨言论，一种办法是向发布这种言论的新闻组不停发送遮断式信息，使得新闻组其他成员一个字都输不进去。另外，一旦查出创办这个新闻组的服务器，黑客通常就能运用基本的黑客策略进行复仇。

在洛杉矶，拉比亚伯拉罕·库柏领导的西蒙·维森塔尔中心长期以来一直在用电子侦察手段追捕纳粹。近来，他们为此广泛搜索了网络，该中心学者里克·埃顿终日在各种键盘和屏幕前度过，他不无几分忧虑地说："极端组织已经学会使用网络，从而大大扩大了和外界的接触。大多数因特网用户对他们的宣传不感兴趣，但你的宣传渠道越多样化，你吸引新主顾的机会也就越大。"事实上，网上新纳粹和其他极端分子的存在的确是个现实问题。在法国，法律禁止服务器散布种族主义言论或者否认大屠杀是历史事实。但在其他西方民主国家，特别是在奉言论自由为圭臬的美国，并没有制订这样的法律。因此，在我们的互联网世界，一位法国网上冲浪者连接上在美国或斯堪的纳维亚的纳粹服务器，实在是件再容易不过的事。由此，不管当地采取什么措施，因特网以其特定形式否决了所有法律限制。前法国大学教授罗伯特·福里森是不承认发生过灭绝犹太人的大屠杀的一班人的领袖，为此引发的法律纠纷使他失去了教职。但福里森在1996年写道："改革之风正朝着修正历史的方向吹，这主要得感谢因特网。20年来第一次，我没坐在法庭里。"利用网络允许播撒所有善恶种子的明显机遇，全球骤然出现了几十个纳粹站点。它们在干什么勾当？1996年，法国犹太学生联合会（UEJF）正式起诉9名巴黎上网服务商——欲上网的个人或公司需通过他们得到服务。这个案子没有什么法律价值（因

为很难强制服务商自己去搜查全部站点和聊天室——可能在那里出现的个人有如恒河沙数)，但它表达出一种深刻的挫折感，并因此成为抗议和社会动荡的重要标志。1996 年 10 月，法国因特网专业人员协会（AFPI）发表长篇声明，特地罗列出它感到有责任维护的权利和义务，从根本上说，就是希望“把因特网的惯例和法规通知给用户”，并希望诸服务商和该协会共同努力，继续保持因特网的正当性。

各国或各地区政府试图限制上网，而世界网络却依然不为所困。与此同时，网上的言论自由往往带着注脚。好战的德国纳粹分子欧内斯特·邓泽尔创建“邓泽尔站点”，就得力于几个因特网组织的支持。这些组织在他们的欢迎页面里对邓泽尔抨击几句，然后却在网页上设置了通向邓泽尔站点的链接。1997 年 2 月 2 日，在法国犹太人最大的一次集会上，犹太人就如何采取合适的措施，反击日益嚣张的否定大屠杀论者、反犹分子和其他种族主义者展开了激烈的讨论。目前，对这些常年困扰人们的问题，还没有一劳永逸的答案。而在此同时，事实表明，因特网正在逐渐地蜕变为一个最新型的避难所，人类最善与最恶的冲动都尽现其中。

第七章 信息战争

战争史也是一门技术史。每个时期都有用来进行大破坏的武器：19 世纪是拿破仑的大军、来复枪、机关枪和战舰；20 世纪初期是坦克和飞机；20 世纪中期是核武器。20 世纪科技上的飞跃不胜枚举。随着世纪末的到来，计算机对军事力量的平衡产生强烈的影响，使我们对武装冲突的构想发生了革命性变化。和从前一样，掌握敌情（“他们计划黎明发起攻击”或“嘿，别把木马带进特洛伊城”）有助于赢得战争。现有系统能够把从卫星以及间谍那里搜集到的情报进行综合处理，赋予指挥员战术上的优势。不仅如此，构筑现代战争离不开计算机系统。

世界大国所关注的内容林林总总，包罗万象。从卫星图像、雷达、国内外计算机运作，直到军用电话和计算机通讯。所有这些情报都对部队官兵有用。不过，也许更令人惊讶的是，它们还用来引导公众舆论支持特殊的军事目的。

但是，信息战有其局限性。它在对抗技术水平相近的敌手，特别是其人民对国内战争记忆犹新的民主政府时，效果更为显著。信息战还能扭转潮流，使之不利于技术最发达的国家。1992年美国发起的索马里行动到1993年却以这样一个象征性的情景黯然结束：一辆叛军军车拖着一位直升机飞行员赤裸的尸体穿过街道，周围挤满兴高采烈的看客。这一场面当即上了CNN有线电视新闻网并传遍整个网络。美国公众舆论一下子就朝着反对索马里行动的方向一边倒。信息战，很大程度上带有老式宣传的风格，仍然能够在网络空间之外发生。一个简单的电视画面，通过卫星播送，便深刻影响了所有观众。

网络即战场

不过，网络空间仍以自己的方式成为战场。自1991年8月联合国在伊拉克发起沙漠盾牌行动以来，这方面出现了许多重大的技术进步。一种被称为沙漠盾牌网（DSNET2）的新网络已投入使用，在实战中一直用来保护超级敏感的数字情报。但是，当时出现的各种创新，并没有都成功地应用于战争之中。在依赖老式通讯手段方面，有个令人震惊的例子，是关于监视伊拉克斯库德导弹的反导弹报警卫星的。一秒钟之内，这一情报不是中转给沙特阿拉伯，而是传到美国科罗拉多州的科

罗拉多斯普林斯基地，该基地再通过电话与保护耶路撒冷和特拉维夫的爱国者导弹群相协调，后者又费了几秒钟时间才在斯库德导弹发射之前发起反击。这种来回兜圈子的系统使得建设新的通讯网络成为当务之急。

五角大楼内部通讯用的是自动数字信息网络（Autodin），并以自动信息处理系统（AMHS）相补充，后者经过特别设计，以便军事信息分析员看到"全球军事和政治趋势的实时图景"。这两个系统都被整合到防卫数据网络（DDN）之中。1995 年夏，五角大楼还决定增设由劳拉公司设计的"国防信息系统－政府开放系统内联档案网络"（DMS—GOSSIP）。在这一领域，军内外设计人员都在以令人眩目的速度取得进展。而海湾战争之前，根本没有人梦想到能用上这些系统。阿兰·凯潘在《第一次信息战：波斯湾战争中通讯、计算机和情报系统的故事》一书中写道："'沙漠风暴'期间，许多用来分配攻击目标和发布战役情况的最至关重要的信息系统，直到伊拉克入侵科威特之日还不存在。它们是技术人员在现场临时设计出来的。技术人员一发现通讯和计算机设备迟迟不到，这些设备的运行范围、工作能力和连接手段又不能满足操作需要，就未经许可，马上另辟蹊径，综合利用军内外各种情报来动手设计网络系统。"

一向由集成网络处理的问题涉及到情报界的核心要害。网络如今是全部军备的命脉所系。就像五角大楼战略计划部门副主任大卫·托德中校明确指出的那样：不

再存在和网络无关的问题。“在今天的电子领域，各个国家、跨国集团和个人都不难接触到具有广泛实用性和相关性的信息。把开放信息源和机密情报源天衣无缝地结合起来，这对保持我们的优势是绝对必要的。最后，我们压制、渗透、贿赂和摧毁对手信息系统的能力显然将改变信息领域的强弱对比。不论使用致命武器还是传统的电子战，都能够阻止敌人得到它自己的情报。美国在信息技术市场上的统治地位已赋予我们军队打信息战争的能力。到目前为止，这种能力拓宽了传统的战争形式。不过，随着信息时代的成熟，将出现真正的革命性的新型战争。信息战将在一种不同的环境里进行，对垒双方将在网络空间厮杀。由于每个潜在敌手都可以接触多重信息系统，战争将以光速在全球范围内虚拟进行。控制网络空间可以减轻对传统武装和火力的需要。”

显然，美国在计算机军备方面不断取得巨大进展，远远甩下了欧洲等地最接近的竞争对手。美国甚至在1995年就开办了一所军官训练学校，专门研究信息战，构思未来的某些数字战场观念。数字战场上的所有伤亡都将是虚拟的，就像置身于一个巨大的电子游戏一样。

美国空军在这方面走在了前面。1993年，美国空军一次性就购买了30万台个人计算机，设立了一个信息战备中心。肯尼思·米尼汉将军当时是空军情报局的情报负责人，他清晰地表述了对他称之为“信息霸权”的看法。米尼汉将军自1995年9月起执掌国防情报局，

1996年2月负责国家安全局。在整个情报界，他的谍报生涯之辉煌罕有其匹，因此他的观点也就格外有分量。米尼汉将军对信息战有自己的一套理论。他说：“信息霸权不属于‘我积累的知识比你的多’之类的线性思维。它不只是用来廓清我方战争迷雾，或加厚敌方疑云，也并非对昨日事件的分析，虽然适度应用历史分析对赢得信息霸权十分重要。信息战有点像是在为争夺空中优势而战。通过它，我们可以提高利用特定信息作出正确决策，并以比敌人更快的速度付诸实施的能力；通过它，我们可以完全改变敌人对现实的理解；通过它，我们甚至可以在敌人睡醒过来考虑今天做什么之前，就利用所掌握的全部知识预测（和影响）明日世界。最重要的是，信息霸权依靠的是头脑，它是把我们自己变成21世纪战场上的强大武器所需要的姿态。”

这种技术紧迫感弥漫在新的美国军队之中，可谓美军的“第二十一条军规”。目前，信息霸权观念占据了美军战略的核心位置。美军在一份冗长但吸引人的《战地手册100—6》[①]（《FM100—6》）文件中，再清楚不过地强调指出：“军队正在迎来新的时代，其特征是信息、信息源和信息散布能力在信息技术支持下加速增长。这个新时代，即所谓信息时代，既提供了独一无二的机

---

① 《FM100－6》1996年8月27日发布于美军网址：http://www.army.mil/

遇，也提出一些艰难的挑战。新的技术将提高我军控制地面形势的能力，后者向来是我国克敌致胜的至关重要的决定性因素。与此同时，新技术也将赋予对手许多同样的能力，敦促军队进行自身改造。”

美军投入了巨额资金研制计算机化战斗模拟技术，这种技术简称为SIMNET，可以通过虚拟交战来训练军队。1991年1月17日，18架AH—64阿帕奇直升机首次进入伊拉克上空，即将发射海湾战争中的第一批导弹，当时机上36人中只有3人过去曾实弹发射过他们所携带的“地狱之火”导弹。这就是SIMNET的训练成果[①]。《在线》杂志在创刊号上为此发表了一篇热情洋溢的文章说：“现代战争运输工具中，大多数人类认知手段都已经要以电子为中介。在‘沙漠风暴’行动中，飞行员和坦克驾驶员都把更多的作战时间用来观察红外线目标显示仪。爱国者导弹发射人员、宙斯盾巡洋舰、机载报警与控制系统（AWACS）雷达工作人员的情况也差不多。战争已经成为美国人通过屏幕观看的一种景观，想要看任何画面，连接上显示器就行。真战场上的真坦克里面可以是模拟的坦克兵，真战场同时也就变成虚拟的。假威胁能够出现在真的雷达屏幕上，而真威胁也能够出现在假的屏幕上。”

---

① 参见《信息优势》，载于网址 http://www.earthlink.net./the-economist/

由此观之，海湾战争可谓是一个非常重要的信息技术实验室，并且衍生出对无数特定领域的研究。海湾战争速战速决，一大特点是伊拉克的伤亡人数不成比例[①]，从而把"信息战"观念展现在人们眼前。海湾战争是首批大规模应用"零阵亡"理论的战争之一。"零阵亡"理论力图创造这样一种战争情境，即通过信息积累，把己方人员伤亡的风险减少到零，虽然这在古往今来绝大多数交战模式中是完全不切实际的。当代许多战争——就算不是绝大多数——其特征仍然是恃强凌弱。强权、贪婪、残暴和恐怖占尽上风。在海湾战争期间，由于伊拉克与对手强弱之势判若云泥，这一理论并未能当真受到检验。而且，沙漠为这种大规模"零阵亡"作战提供了完美的舞台，绝大部分攻击都可在"安全距离"之外发起，远离大多数伊拉克武器的射程。

信息战建设在继续进行。1995年7月，法国首次发射间谍卫星。这颗名叫赫利俄斯（希腊神话中的太阳神）的卫星从圭亚那的库鲁腾空而起，进入太空轨道，使法国得以跻身于技术大国俱乐部。现在，法国人很大程度上就和他们的美国同行一样，被淹没在信息汪洋大海之中。他们只能检查所有搜集来的图像的百分之一到百分之十。这些图像实在太多了，分析不过来。

---

① 至今没有公开的确定的统计数字。据估计伊拉克方面死亡人数在4万至20多万之间，联合国军队有340名官兵死亡。

那么，这种技术意味着什么呢？凭这么一颗卫星及其搜集来的情报，法国就更加强大了吗？前中情局特工、美国战略学家爱德华·鲁特维克现在在战略和国际研究中心（CSIS）工作，主持关于中情局经济谍报活动的研讨。他最初呼吁各民主国家向波斯尼亚人提供武器和军火时[①]，可能还存心引起争议。但他说下面这番话时则绝对是有的放矢："今天的发达国家人口更多，家庭更小。没有哪个发达国家会只为抵抗对第三方发起的侵略，而承受重大战争伤亡。这就把这些国家的武装部队置于一种特殊境地：虽然一如既往地热衷于获得最高预算额度，可能甚至更热衷于费用高昂的演习和训练，以保持'高度战备状态，但完全不准备抗击享有善于反击的声誉的侵略者。'"

尽管科技发展有如魔术般迅速，战争的残酷程度看来恐怕和古代并无二致。美国未来学家阿尔温·托夫勒在《第三次浪潮》中所描述的那种拥有先进技术的军队，在索马里、前南斯拉夫、车臣以及全球其他热点地区的行动都没有达到目标。虽然如此，世界各国军队都在坚持不懈地为信息战争作准备。信息战，不管目前有何不足，终将得到发展，并表现出种种优势。

---

① 到1995年11月底，美国决定投入4亿美元，开始"行动训练和设备"计划。到1996年12月，这一计划已向波斯尼亚穆斯林提供了45辆战斗坦克、80辆步兵战车、15架直升机和46万进攻型武器。

首先，“虚拟”敌人要比真实的敌人更加活跃。在战争中，他们丝毫不涉及到因部队调动而产生的麻烦的后勤事宜。他们所需要的一切，不过是一杯可口的咖啡和用来袭击海滩的计算机键盘。信息战（无人在战争中死亡）的另一优点是它通常在经济战场上展开。苏联解体以后，世界主要国家就在经济战场上展开争夺。扎基·赖迪有言：“民主国家之间的战争是不可思议的。”眼下是多少个世纪以来头一回，在主权国家之间没有发生战争——最近的一次是 1995 年秘鲁和厄瓜多尔之间爆发的一系列短促的小规模武装冲突。如果我们接受这一事实，以之佐证赖迪的看法，那么，我们也必须明白，人类从来没有放弃，也没有遗忘过战争。1945 年以来世界上发生过 25 起大规模武装冲突，每起都导致每年至少 1000 人丧生（1994 年，仅在卢旺达就有 50 万人被杀）。各工业化国家以及联合国在制约因宗教、民族主义或领土要求而爆发的战争方面，一直都是无能为力的。这类冲突中，有许多都发生在不同派别原本和平共处的地区，但结果看来是一样的：大屠杀发生、妇女遭到军队强奸、家庭失所、骨肉流离、社会生活百孔千疮；城市破败、土地荒芜、疯子和屠夫侵犯着人权。

在工业化大国，高科技侦察手段无孔不入，出现了爆炸式发展；但因特网的存在还不能遏止地区战争，残暴的武力对那些草菅人命、藐视言论自由的人来说仍然有用。这和相信因特网很快就会产生重大影响并不矛

盾。眼下，按照纽特·金格里奇的好友阿尔温·托夫勒的说法，所谓的发达国家有着别样的困扰。托夫勒说："当然，第三次浪潮'之后的国家'依然需要能源和食品，但他们现在也需要可转化为财富的知识。他们需要获得或者控制世界数据库和电讯网络。他们需要市场来营销信息密集产品和服务、营销金融服务……管理咨询……软件……电视节目……银行业务……储备系统……信用资讯……保险……制药研究……网络管理……信息系统集成……经济情报……培训系统……模拟……新闻服务……以及所有他们仰赖的信息和电讯技术。他们需要保护知识产品不受盗版侵犯。"

军队在行动

凭借因特网优势，当代资本主义正在以光速向前发展，没有显示出任何放慢速度的迹象。这至少得部分地归功于首先开发网络的美国军方。不过，这样迅猛的扩张和发展已表现出某些变化。尽管是五角大楼和国防高级研究计划局（DARPA）在1969年首次创立了计算机网络国防高级研究计划局网（ARPANET），但该网络迅速普及开来，意味着它再也不能用来传输美国最敏感的资料——不论加密与否。美军方仍然保留国防高级研究计划局网（ARPANET）作研究之用，并为非军方人士提供了NSFnet。

美国中情局为下属情报机构专门设计了一个新的、专业化的全球网络——内连网（Interlink）。内连网自1994年12月起投入使用，被中情局认为是固若金汤的堡垒。中情局因而将其虚拟王冠上的珠宝——国家侦察署间谍卫星所搜集的数字图像都储存在里面。五角大楼的因特网址（全部以“. mil”结尾）则用来储存不重要的信息。人们可以从保护措施很少的军事网（Milnet）[①] 里看到。所有机密电子邮件都禁止进入因特网。五角大楼也设有自己的网站[②]，每一主页上都刊载着同样的警告：“安全和保密注意事项：1. 本站点提供公共服务，由美军指挥、控制、通讯和计算机信息系统（DISC4）主任设立。2. 本站点旨在供公众用以浏览和检索信息，并仅限于此。3. 严禁未经授权上载或更改本项服务中信息的行为，并可能根据1986年计算机欺诈和滥用法予以处罚。4. 有关您来访的统计资料和其它信息均被记录。5. 本站点所有信息均被认为是公开信息，可以传布和复制。”

物换星移，五角大楼成为它称之为“网络战”的信

---

① 军事网Milnet最早是高级研究计划局网（ARPANET）的一部分，两个网络于1984年分开，ARPANET现在专门用于研究。

② 国防网：www.dtic.dla.mil/defenselink/ 美国陆军网：www.army.mil/美国海军网：www.navy.mil/ 美国空军网：www.af.mil/ 美国海军陆战队网：www.usmc.mil/ 另外，加拿大军队网：www.cfcsc.dnd.ca/links/milorg/usf.html

息战的原动力之一。很多人不知道，海军陆战队也对战略理论深有研究，甚至也在注意有无可能影响他们军事行动的新威胁。移动电话的发展、南美种植毒品的叛乱者对移动电话的利用，都一直是大量军事研究的课题，虽然这类技术的局限性已经暴露了出来[①]（位于恰帕斯州的墨西哥游击队大量散发因特网消息，没过多久，这些消息里就混入了与真实消息数量不相上下的假消息和错误消息，破坏了副司令员马科斯的公关战）。

1995年6月6日，在华盛顿召开的一个研讨会上，美全军高级监察机构——指挥、控制、通讯和计算机系统——主任阿瑟·采布罗夫斯基估计，1996年美国花费了10亿美元用于保障军用计算机安全。采布罗夫斯基解释道，基于未来可能发生由某个敌对大国操纵一群黑客发起大规模攻击的“电子珍珠港”事件，美军思维方式逐渐有所改变。他说，冷战时期，常规核武器袭击威胁着全球；而今，各国渐渐转而担忧虚拟的世界决战，这种恐惧是可以理解的。不妨看看来自离会场一英里之遥的其它论据：军事预算甚至可能会因这一新威胁而增加。

安全问题促使有关决策人开发出专门针对信息时代而设计的新型计算机化军用网络。美国军方和普通百姓

---

① 参见网址：gopher：//ossnet中阿尔弗雷德·格雷将军所撰《90年代的全球情报挑战》一文。

一样，日益频繁地使用电子通讯，但把安全放在更优先考虑的地位。美军现在使用的计算机超过210万台，区域性网络达1万个，长途网络100个。兰德集团公司委托进行的一项研究指出，军事网络的增长迫使人们要彻底重估美国的军事战略。研究报告讨论了其它种种因素，同时指出："信息战没有前线和后方。网络系统所允许访问的任何地方都是潜在的战场。当前的趋势表明，美国经济将日益依赖于错综复杂的互连网络控制系统，以满足诸如石油和天然气管道、电子线路网等等的需要。这些系统的脆弱性目前人们了解得还很少。另外，威慑和报复手段也不确定，除信息战威胁之外，可能还得依靠传统的军事干预。总而言之，面对外来攻击，美国本土恐怕不再能高枕无忧。[①]"

据管理五角大楼全部网络的国防信息系统局（DISA）估计，1995年美国军用计算机遭受了325，000次攻击，其中每150次攻击中只有一次被检测到和向上报告。该局说："大量国防工作受到妨碍，包括武器和超级计算机研制、后勤、财政、采购、人员管理、军队保健和工资发放。"美军在规划未来的全球电子通讯架构时，必须把所有这些因素都考虑进去。1996年，国防信息系统局成立全球行动和安全中心，负责集中关于国防部所受袭击的所有情况，从而让五角大楼掌握重要数

① 参见兰德公司网址：www.rand.org

据。不仅如此，在网络基础设施方面，五角大楼也有大动作。它首创了 DISN 全球支持服务，预算 20 亿美元，业已交付波音公司执行。在未来几年里，五角大楼通过被称为 C^4I（指挥、控制、通讯、计算机和情报）的网络系统，将可以分享“声音、数据、图像和信息系统，同时还保证安全。”1996 年 10 月，国防信息系统局发表“任务需要声明”指出：“至关重要的 C^4I 信息传输必须有能力畅通无阻地连通全球，规模可大可小，供应可随机应变，能轻松延伸到世界任何位置，能接受含技术及附加值服务以满足未来战役要求[①]。”

约翰·多伊奇在 1995 年受命担任中情局局长之际，就对这些问题有了更多的思考。他成立了一个部门间智囊团，负责制订改善私人和政府电讯安全，以及计算机网络所需要采取的措施（“人人都说这是个大问题，得花数十亿美元解决它，但过后就闭口不谈了”）。对多伊奇来说，纵然一时没有立竿见影的解决办法，也要努力把所有问题摊到桌面上来讨论。

迄今为止，还几乎没有事实能表明美国对外来袭击的担忧不是杞人忧天。五角大楼肯定地说，它曾几次遭到黑客的猛烈攻击，并公开承认害怕病毒进入其服务器。但不管怎样，五角大楼也承认，这些黑客袭击的目标都是 Milnet 之类最脆弱的系统，这些系统没有得到严密保

① 国防信息系统局网址：http：//www.disa.mil/disahome.html

护，也不包含任何敏感信息。但问题依旧存在：黑客过去是怎么渗透进军方计算机的？他们现在又是如何进入的？五角大楼一直封锁黑客攻击的详细情况，因为它希望把黑客攻击减少到最低限度，转移人们对军用计算机系统的薄弱环节的注意力，或者也是为了使军用计算机系统在公众眼里显得更加重要，从而佐证其预算之合理。1996 年瑞典黑客对中情局网站的袭击就是一个有趣的例子。这件事弄得中情局十分难堪，可是要紧的信息根本就没遇到危险。1996 年 5 月，在前面提到的美国总审计局的报告中，分析家们强调指出，1994 年 3 月和 4 月发生的英国黑客袭击美空军罗马（纽约）实验室事件则是个完全不同的问题，而且可能带有犯罪目的："空军官员告诉我们，至少其中一名黑客可能一直在为另外某个对获得军事研究数据很感兴趣的国家工作……另外，这些黑客可能曾企图在软件中安放能在几年后启动的恶意编码，它可能会危及武器系统安全操作的能力，甚至威胁到操作这一系统的士兵或飞行员的生命。"

五角大楼的行政机器高速运转起来，一心想要在第一时间对最糟糕的情况作出反应。1994 年 2 月，专门处理黑客事件的自动化系统安全事故援助小组（ASSIST）成立，下设特别机构信息系统安全中心，并得到了和国家计算机安全中心紧密合作的国家安全局的技术帮助。1994 年在华盛顿召开的一次研讨会专门讨论了计算机不良行为对美国安全造成的威胁。司法部下属的计算机

犯罪署负责人斯科特·卡尼在会上敲响了警钟。看来，令人深感忧虑的是黑客受到诱惑，不再从事计算机恶作剧，而是被犯罪组织所重金收买。卡尼说：“过去，情报放在保险箱里，保险箱再上锁，我们再锁住整栋房子，外面围道篱笆，再派警卫以确保（情报）安全。现在，我们把敏感的情报放在网上，接着就舒舒服服地休息了，因为房子外面有篱笆围着。”

美国军事官员正以美国及美国公民安全的名义，拨出大量资金打击虚拟的入侵者。不过，既然最好的防卫就是适当进攻，看到美国充当攻击者的角色，用病毒和逻辑炸弹破坏敌对系统，也就用不着大惊小怪。无论如何，至少在最近的将来，黑客看来还有得可忙的。

第八章 因特网和谍报经济

一和欧洲空中客车工业集团提起因特网，他们就怒不可遏，认定主要竞争对手波音公司利用因特网攻击了他们。

事情得从网上发布的一份空难报告摘要说起。1988年6月25日，Absheim A—320飞机在一次航空展中进行惊险的飞行表演时，失事坠毁，造成4人死亡，100人受伤。问题是有关事故报告尚未公开，网上却出现了该报告的摘要，而且其中为空中客车公司辩护的部分被人别有用心地删除了。紧接着，一批抨击空中客车及其合作伙伴法国航空航天工业公司的恶意信件突然神秘地出现在讨论航空和运输的新闻组里。

因特网：错误消息的理想载体

在法国航空航天工业公司，有些热心的雇员也是网上冲浪的高手，一直都很有兴趣地注意着这些新闻组。

一方面是出于爱好，另一个原因却是法国航空航天工业公司很早就认识到，这些新闻组乃是“识别本行业专家和评估新技术与市场竞争的实用工具。”这些雇员发现所在公司遭到恶毒攻击后，深感诧异，于是开始追查信件作者。没费多大劲，他们就找到了发送信息的原始地址和全球普通代码。不幸的是，进一步检查表明，所有地址及其包装都是假的。对懂尤尼克斯操作系统的人来说，造这种假一点不难。这些信件真正的来源地是美国，作者利用了芬兰的匿名服务器对其进行假包装。根据对包装的分析，法国航空航天工业公司强烈怀疑波音公司就是在网上发动大规模错误信息战的始作俑者之一。

不过，新闻组不仅可以被用作攻击手段，也可以被商界用来搜集信息。下面是来自航空业的另一个例子：1994年万圣节前夕，一架ATR客机[①]在美国坠毁。在事后的安全调查期间，ATR飞机全部停飞了两个月。从商业上说，这个决定是灾难性的——损失两个月收入。停飞期间，各专业新闻组，包括计算机服务公司（全美最大的在线信息服务机构之一）的AVSIG新闻组，都就此争论得热火朝天。

当时，网上支持欧洲飞机制造商的贴子寥寥无几，

① ATR是一家大型欧洲航空联合企业，包括意大利飞机公司、法国航空航天工业公司和英国航空航天公司，其下属飞机统称ATR。

数目远低于反对派。1995 年 1 月的一天，一位给航空业某一定期出版物写稿的记者在新闻组张贴了一个不起眼的贴子。他问道："我听说飞行限制将要取消，请问有谁能证实吗?"很快就有人作了肯定的答复。接着，仅仅三天之后，ATR 收到了许可他们复飞的正式决定。假如 ATR 一直跟踪新闻组讨论，他们原本可以一下子提前三天复飞的。

新闻组还是搜集经济情报的一个源泉。有些事件可能对某公司或某国家的存亡产生特殊影响。花费巨额资金来搜集和积累有关情报，现在已开始证明是值得的。许多人断言，经济业已成为民主国家的新战场。不管这是真是假，可以肯定地说，在今天的商业环境里，掌握信息乃公司成败之本，而因特网则是达到这一目的的基本手段。

另一家不得不应付网上负面舆论的法国公司是石油巨人托塔尔。当时，法国已投入巨额资金在缅甸建精炼厂，托塔尔石油公司正准备在缅甸开发一处巨大的海底天然气油田。但问题来了：诺贝尔和平奖获得者、缅甸人权斗士昂山素季反对这个项目。理由是：该项目将会而且只会让她和她的追随者长期反抗的专制的缅甸军阀赚大钱。她要求停止实施这个项目，要求托塔尔石油公司离开缅甸。这个要求是完全合乎情理的。南非的纳尔逊·曼德拉在反抗种族隔离制度时，也对形形色色的公司提过类似的要求。在各种因特网新闻组（如 soc.cul-

ture. burma）以及包括全球投机家乔治·索罗斯的网站在内[1]的各种非政府的好事的网站上，托塔尔石油公司都被骂得体无完肤。淹没在因特网舆论海啸之中的托塔尔石油公司则和国际人权联盟取得联系，力图向国际人权联盟以及全世界证明他们没有剥削任何人，他们的投资对缅甸老百姓有益无害。托塔尔石油公司还掏腰包请了法国及世界各国许多记者飞往缅甸实地考察。当然，并没有多少有新闻价值的东西可看。深明因特网奥妙的咨询顾问则把托塔尔/缅甸事件当作试验案例，为托塔尔石油公司策划了反攻战略。这些顾问甚至隐名埋姓亲自上阵，反驳对托塔尔石油公司的攻击。因为他们相信，网上的反对之声乃是英美试图把托塔尔石油公司赶出缅甸的阴谋。真实情况要远比这错综复杂得多。1997年3月，美国国会就对缅甸的政策展开激烈争论：美缅应该断绝经济关系吗？美国应该效仿法国继续在缅甸投资吗？围绕种族隔离制度下的南非，也曾发生过同样激烈的政治论争，但这次观众更多。好也罢，坏也罢，现在不论什么人，有台计算机和调制解调器，就能进入讨论圈子。

---

① 参见自由缅甸网址：www.irn.org/burma/total.html 索罗斯基金网址：www.soros.org/burma/fmtotal.html 托塔尔石油公司网址：www.total.com/fr/cahier/yadana.html

信息：秘密武器

谁申请了聚合物的最新专利？这位学者属于哪个研究组？还打算呆在那儿吗？前俄罗斯总理安德列·科济列夫 1985 年以前作过什么旅行？谁是航空隐形技术领域首屈一指的专家？从现在到 20 世纪末我们对巴西汽车市场能指望些什么？这些问题的答案全都以数字形式存在，对那些需要立即得到答案的人来说，它们就是财富。

当今世界，信息即武器。信息就在美国及全球 5000 多个在线数据库中。这些数据库里有数以百万页计的博士论文——任何想象得到的题目都有专题论述；还有来自世界各个角落的科学出版物。它们已经成为非同小可的人类知识宝库。利用关键词或者整个文本，雅虎之类的搜索引擎就能够扫遍浩瀚的网络，查找到大部分信息的所在位置。只要交一点费用，诸如 Dialog 和 Lexis/Nexis 这样的大型数据库就会公布成千上万的出版物的内容。不上网的一流纸质国际出版物越来越罕见，何况这几乎不花它们什么钱——文章都是早就写好的，而且就在计算机里。在网上数据库里查询文章，每个文本收费从一个美元到几个美元不等，所以重大研究所费不赀。这些数据库虽然已经存在一段时间了，但它们的全部潜力还有待发掘。极其复杂的分拣程序能够熟练地

操纵数据库，从中提取和分析有效信息。最早对这些分拣程序感兴趣的就是谍报机构。

毫不奇怪，美国中情局在这方面一马当先。他们为这些分拣系统投入了大量资金，目的是要在最短时间内处理尽可能多的原始数据，分析并取得别处找不到的敏感细节。最早开发网络的五角大楼国防高级研究计划局在70年代就率先开始研究这个课题。起初，分拣系统只处理简短单纯的信息和内部备忘录；后来，它们也能够把通讯社的在线报道自动分发给有关各方。美国研究人员再接再厉，开始处理数据库中大量有效信息，力图开发出迅速、方便、节省时间的研究手段。这期间出现的搜索引擎“主题”（Topic）迅速成为了数据库研究的一项行业规范[①]。尽管“主题”引擎最初只限军方和谍报机构使用，但它仍然迅速成为一项基本的研究工具，被整合进无数公司的软件之中。

要处理大量信息输入，没有搜索引擎是无从谈起的。原子能委员会针对自身的特殊需要开发出“疾跑”（Sprint）软件，能够管理和自动分拣各种语言的文本。另一个网络研究分析软件名叫“泰加”（Taiga），是由汤姆森计算机公司的克里斯蒂安·克鲁梅为法国国外安全总局研制的，其设计初衷原本是为了搜索前苏联数据库。只是到不久以前，“泰加”软件才获准在非政府范

① 网址：http：//verity.com/products.html

围使用，每弹出一次约要4万美元。现在，“泰加”软件归迈迪西亚公司（Madicia）所有和开发。法国电讯的分公司Questel收购了迈迪西亚公司，又于1995年春试图以100万美元左右的价格把它卖给美国国际商用机器公司，但由于法国公众舆论以国家利益为由一致反对，这项交易终于作罢。“泰加”最后被卖给IPSIC，后者更名为Taiga Noemic。Noemic即“泰加”的升级版本，主要是法国军事情报指挥中心在用，后者看来对它是万分满意。

Noemic/Taiga能够自动合并数据和处理任何语言的文本，不管它们是在数据库里还是来自新闻机构。如果“泰加”用户对种植胡椒感兴趣，这个程序就会自动搜寻和分拣所有可用的网上信息，以及通讯社消息和数据库里的文章。它能够克服棘手的语义和语言学障碍，并列和首语重复法也难不倒它。它可以变戏法般地轻松改变修辞，跳过语言历时分析，面对只出现过一次的生僻字眼胜利地哈哈大笑。年轻的科西嘉程序员帕斯卡·安德雷进一步扩展了“泰加”的指令表，除原来着重的地缘政治学之外，还把技术分析也包括进去。“泰加”的工作原理是把所有待分析文本（自动）翻译成中间语言，然后再用程序加以分析。举个例子来说，假定“泰加”收到这么一条消息：“空中客车A—320正在飞往亚洲。在的黎波里上空某处，机上发生炸弹爆炸。阿尔及利亚国防部长身亡。”眨眼之间（以每秒10亿字符的速度），“泰

加”程序就把这条消息翻译成如下中间语言：

“be - tch - dpl - air/cmc/airb/a320，be - loc - pol - vil/cap/lby，ag - phy - vlc，bpp/bpf - min - def \ alg.”

“泰加”自有一套数据辞典进行对等翻译：空中客车 A - 320 被泛泛译成“技术产品”（be - tch），“在空中移动”（dpl - air），“商业”（cmc），爆炸被译成“具体的暴力行动”（ag - phy - vlc），如此等等。

由于“泰加”深通语言微妙幽深之处（隐喻及婉转的表达法），它不仅能译出词句的意义，而且能表达出思想观点的演进。使用“泰加”不需要关键词：中间语言所确定的措辞可以用普通概念（飞机和直升机）加以重新组织，而古典的关键词（不论飞机或者直升机）是不能包含这些普通概念的。在上述例子里，搜寻“be - tch - dpl - air”就能检索到这两种飞机。

帕斯卡·安德雷解释起他的小小杰作的工作原理，从来都不惮其烦：“归根到底，一开始就要使用高水平辞典，以便理解人们将要研究的领域所使用的专业词汇。虽然有一些好辞典可用，但（‘泰加’）辞典的绝大部分都是我们自己编辑的。”为此，经常需要求助于人工智能技术，请认知专家把专门技术“下载”到“泰加”里。同样地，以胡椒种植为例，“泰加”程序需要请一位园艺专家来就胡椒种植编写一本带术语表的中间语言辞典，以便获得显著的搜寻效果。

持否定态度的人有时把说“不”当成了一种责任。

某些法国国外安全总局官员就觉得“泰加”太复杂了。还有人说“泰加”在90年代初期是非常有意思的解决办法，但后来就落到了竞争对手的后面。但不管怎么说，对懂得如何使用它的人来说，“泰加”是最强大的工具。1996年年底，克里斯蒂安·克鲁梅开始出售“泰加”的升级版，取名Noemic。新版本使用了更加复杂的语义控制技术。

假如法国国外安全总局监视整个网络及网上信息还存在某些困难，说它努力不够是不会弄错的。法国人对新闻组最感兴趣。专攻“高级信息”的软件早就被用来处理重要的数字通讯流动——就连被合法或非法截听的数字电话通讯都被数字化，并译成了中间语言。这初听起来可能有点奇怪，实际则顺理成章。1994年1月的一次电视曝光后，德国联邦情报局一位官员承认，他们的计算机信息部门一直就在专门研究计算机情报。与此同时，据悉德国联邦情报局还找到了加强其辞典数据库的办法，从而可以自动倾听和分析被截取的电话通讯。

1995年上半年，法国军事情报指挥中心买下了几十个“泰加”工作站。通过运行和美国家安全局所用颇为类似的软件，法国军事情报指挥中心大大扩充了它自动窃听和分析因特网的能力。比如说，有两位计算机服务公司客户都住在巴黎，如果其中一位向另一位发送电子邮件，邮件总得通过美国俄亥俄州哥伦布市的一个节点传送，那儿有计算机服务公司的大型计算站。因此，

电子通讯就算具体地址都在当地，实际运作可能仍是国际性的；而且，邮件传送经过美国，增加了美国家安全局的截听机会。

对关注信息分析的人来说，因特网不啻是一道通向金矿的彩虹。鼓励研发“泰加”这类软件的人士相信，在战略信息、侦察技术以及经济信息等领域，迄今无从获悉的大量经济活动，不久就会暴露在监视者眼皮底下。这类信息渠道将给公司内部守法（或不守法）的专业技术人员，或者谍报机构带来难以置信的财富。通过设立信息过滤装置和语义分析步骤，我们能够从大量原始数据中自动产生出新的信息。

汤姆森计算机是最早开发“泰加”的公司之一。该公司自己开设了一个名叫 GRIT 的侦察技术网络，使用的是美国中情局的“主题”搜索引擎。代销中情局程序的 Verity 公司在一本促销小册子上说，“主题”软件能每月分拣来自数据库、光盘和磁带的两万到三万份新文件：“本公司的每位订户都按月收到对应于他们所关心领域的摘要选录。这些摘要被称为研究简介，由负责挑选和刊布信息的研究人员预先严格划定范围。”不论哪个国家的大型军火公司都很高兴得到这么一个有效手段，从而掌握军火业的最新进展情况。中情局软件开发人员的辛勤工作使得“主题”软件成为一项行业规范，全球有一万多家公司在使用它。“主题”的新版本“主题网络搜索者”（Topic WebSearcher），特别适合在网上

查找信息并为之编写索引。在这个领域，谁能开发出最简单、速度最快的界面，谁就可以获得巨大的经济回报。另外一个搜索引擎名叫雅虎（Yahoo）[1]，是两位非常聪明的学生——大卫·菲洛和杰里·杨（杨致远）——一起搞成的。菲洛和杨致远都是斯坦福大学电子工程系在读博士。1994年4月，他们开始建设自己的数据库。目标很简单，就是把散布在网上的他们感兴趣的站点加以整理，以便他们更容易操作和驾驭。慢慢地，他们的系统越做越大，成千上万的网民潮涌而来，通过他们的系统上网冲浪。两人于是开始针对自己和广大网民的需要进一步开发软件程序，最终雅虎成为万维网上最主要的搜索引擎之一，其地位相当于同一时期卡内基一梅隆大学研制的来科思（Lycos）搜索引擎[2]。TriVium公司（由经济学家理查德·科林主持）开发的Gingo程序的概念层次则更高一筹。Gingo研发人员来自各个学科，和米切尔·塞雷斯关系密切，成员包括数学家兼社会学家米切尔·奥捷和哲学家皮埃尔·列维。Gingo的设计宗旨是："驾驭复杂的信息系统"和"掌握发展中的虚拟经济领域"。比如说，某一公司想要绘制全体职员的技能图表，Gingo就会创制一份"知识树"图表，其中每个职员都被指定一个位置，在那里，该职员所掌握的全部

① 网址：http：//www.yahoo.com

② 网址：http：//lycos.cs.cmu.edu

知识都可立即用直观化的图表形式表示出来。这类程序还能够直观地显示可不断自动更新的各项信息的连续变化。Gingo 软件可以让公司掌握前所未有之多的信息，在此前不可想象的复杂分析的基础上作出战略决策。法国人率先开发的另一个系统是“伯里克利”（Pericles，古雅典政治家）。它是创建 Datatops 公司的一群前海空联合飞行员研制的，目的是通过分析网络信息，去芜取精，把有效信息提供给客户。由于人们交口称赞，到1996年，“伯里克利”程序开始赢利，但其它许多公司也在争夺这个新兴市场。法国人克劳德·维格尔和美国人斯坦森·盖尔在美国加利福尼亚州合资建立了 Semio 公司，并于 1997 年 2 月推出 Semiomap 搜索引擎。它借助功能强大的图形界面表示信息，把文字和图像连在一起。美国得克萨斯州科珀斯克里斯蒂的 Psytep 公司则使用戴尔芬的 Infopower 程序，为五花八门的公司准备报告，向它们提供有关其独特的竞争环境的详细情况，从而提高了这些公司的灵活应变能力和竞争能力。Psytep 因而大获成功。所有这些软件工具都大有新的用武之地。

除 Infopower 外，DR—LINK（通过语言知识检索文件）也是美国人开发的程序，它可以从不拘何处的数字数据库中提取信息。制作 DR—LINK 的 Textwise 公司是由原先在兰克复印机有限公司工作的迈克·温纳和锡拉丘兹大学计算机学家伊丽莎白·丽迪共同创办的。多年

前最早资助因特网的美国防高级研究计划局也通过情报界人士发起的“告密者”组织为 DR - LINK 的开发提供了资金。这些软件各有其专长和特殊功能，但仍然抵御不了新程序进入市场所带来的冲击。市场上似乎每个星期都有新的软件露面；另外，如果不提 SRA 国际公司和 Isoquest 公司推出的 Netowl 和 NameTag 的话，这份工具软件清单就有欠完整了。

所有这些软件都能单独处理正在大量繁殖的连接全球的服务器，把其中内容编写出索引，逐日分析所有新增信息，从而使用户了解到最新情况。说起全球万维网址的总数，任何估计数字都注定不可能准确。但美国麻省理工学院学者马修·格雷在他的 1996 年“因特网增长总结”中仍然给出了近似数字：1995 年 6 月，23,600 个网址；1996 年 1 月，100,000 个网址；1996 年 6 月，230,000 个网址，1997 年 1 月，650,000 个网址——12 个月内增长 20 倍[①]！每个搜索软件都能识别几乎所有全球万维网服务器，把每天出现的成打新站点编入索引并加以分析，使用户能够找到它们。网上通行的各种引擎展示了网络的非凡威力，充分表明一个新的时代已经来临——过去需要在图书馆花上几天几星期查找的资讯如今唾手可得，而且毋需费力，毋需等候，其深度和广度

---

① 参见网址：http：//www.mit.edu：8001/afs/athena.mit.edu/user/r/e/rei/wroot/people/mkgray/net/

前所未有。这并不是说我们的图书馆有朝一日会像古希腊的亚历山大城一样消失，这些图书馆不是需要保护的濒危物种；但显而易见，它们的作用会发生变化。图书馆很快就将成为虚拟结构，可以通过因特网入内浏览。

当然，困难肯定是存在的，这些困难甚至就来自于显著的进步。以 1996 年上半年问世的 Dejanews 搜索引擎为例，这个引擎能够从因特网上所有新闻组里搜寻出单个字词或名称，它迅速、有效，而且可靠。如果你想知道邻居的情况，几秒钟之内，Dejanews 就能遍查几个月来的聊天对话，列出你邻居名字历次出现的情况。然后，人们因之起了惊慌——只要点击这个名字，你邻居登录上网的次数、他所偏爱的话题、他参与哪些交谈、他回应哪些信息，所有这些统计资料你便一目了然。许多搜索引擎还具备另一个功能，被称为“魔法小甜饼”。“魔法小甜饼”向服务器提供它认为有用的客户资讯，其中可能包括客户登录上网时间、所访问的聊天室、在聊天室里消磨了多少时间、用户计算机型号、甚至用户软件的名称。服务器拥有这些资讯后，就能把它认为合适的广告和促销单发送给客户。更有甚者，这些资讯可以出售给期望向预经筛选的潜在买主直销的公司或服务商。结果，关于登录上网者表现的大量资料不断遭到编辑。不过，现在高兴起来吧，网络依然如故（一个自治的乌托邦），网络仙女们已经创造出“小甜饼怪物”，不让魔法小甜饼被坏罐子收走。这听起来虽然好像直接来自奥

威尔的小说《一九八四》，但可绝对不是坏消息。

令人惊讶的是，使用这些搜索引擎不必交钱。人们如此依赖这些引擎来漫游因特网，本可能有人指望从中渔利，尤其当信息没准远在半个地球之外某个异国大学的计算机里，而这些引擎则是得到它们的唯一工具的时候。然而，正是这种免费的信息交换，令每个人面对因特网都兴奋莫名，满心憧憬着信息高速公路把我们带往个人自由的新时代。不幸的是，看来高速公路以后也将收费，或者说，有些公司是这么希望的。

高级信息：用户指南

法国人倾力开发高级信息“产业”，为此投入了国家侦察中心（法国的联邦调查局）的部分人力物力。法国国家侦察中心还定期组织为期一周的研讨会，有150名法国专家出席，相互交流和讨论这一领域的最新进展。最近一次研讨会是1995年5月30日到6月2日之间召开的，专家们在会上谈到的东西引起世界一流大公司的关注。罗纳—普朗公司、法国航空航天工业公司、原子能委员会、法国电力公司、国际商用机器公司、欧莱雅、合成实验室公司、米什兰公司等许多大公司都派代表与会。

为深入理解编订信息的用途，我们可以看看这个例子。比方某化学公司的一群红外显微镜技术专家想通过

使用搜索引擎，了解还有谁也在研究这种非常特殊的高科技技术。他们使用办公室计算机（其硬盘可能需安装类似于某研究所开发的 Dataview 搜索引擎的程序）登录上网，访问一个名叫“化工摘要”（Chemical Abstracts）的美国数据库，这个数据库里囊括了化工方面 1500 万篇文章。这些技术专家们首先寻找有关红外技术的文章，然后再把范围缩小到与他们的课题最相似的研究著述。再不会有比这更方便，或更详尽的调查了。

法国图卢兹的伯纳德·杜塞开发的 Tetralogie 软件令人拍案惊奇。对经常访问数据库的人来说，在研究某个科学课题时，一次分析 5000 到 10,000 份文件根本是司空见惯的寻常事。分析首先从网络搜寻开始，找出最合适的在线数据库，然后，非常迅速地，原始数据就开始以多维图形的形式出现在工作站的屏幕上。在科学界，学者通过研讨会交流就和在科学杂志上发表文章一样，乃是科研活力的源泉。很多情况下，这些文章似乎就是一场场微型研讨会，因为作者通常是一群科研人员，而不是某人单枪匹马。Tetralogie 的主要功能就是在知道某一给定领域的研究者名字之后，将他们链接在一起，分析他们的各种关系。Tetralogie 先对数据进行加工，把每个人每一事项都用不同色彩加以标记或分类，为每个研究者指定一个单独的点，将各种色彩聚集在一起。这样，操作者就能通过生动的图像看见谁一直在合作，谁在单干，谁有可能被笼络到自己的研究小组。伯纳德·

杜塞在演示程序时解释说："显然，我们看到的是这个领域的重要人物。其中有些人牢牢控制住手下工作人员，哪儿都不让他们去；另外一些人则到处跑，为谁工作都可以。就这么简单。在召开研讨会之前，如果你研究一下这个图，只消两分钟左右就能知道你想邀请的头四到五位研究者是谁。"

图阿费克·德卡基对 Tetralogie 软件做了正式说明[①]："用来构成这些协作网络的信息来自著书目录式结构的数据库。我们可以通过这些正式网络发现潜在的合作者，检测到孤立的研究小组，了解技术进展情况。"更通俗点说，熟练的用户能够凭借这个软件发现科学界里心存怨怼、牢骚满腹之士，了解谁可能接受其它工作机会，谁又可能拒绝。Tetralogie 甚至不费多大劲，就能找出显要人物所力图牢牢把持的给定团体中的"隐形"同事。"当名字出现在它们不应该出现的地方，你就能断定这一点。"显然。设计这个软件的目的在于搜寻更准确、更有竞争力的信息。"首先是搜集信息，经过一系列步骤，最后作出决定。"不管对公司还是谍报机构(或者二者合一)，Tetralogie 都已成为招募专业人员加盟的有用工具。

现已开发出的其它软件为用户提供了不同的选择机会。对专业人员来说，这些软件性质是一样的，它们都

---

① 参见网址：http：//atlas.irit.fr/

有能力尽可能迅速地获得给定服务器或数据库的基本内容，或者搜索某一给定新闻组的所有对话。“疾跑”程序可以自动把庞杂的在线信息（每5分钟5000万8比特组字节或3.3万页）编入索引。这些文本要么来自包含简短的著作“摘要”的结构文本数据库；要么来自包含原始数据（化学方程式、实际科学数据）的“结构”(Structurals)。再经语言学家一番雕琢，这些专业化软件程序便可搜索新增加到数据库的词汇，以及使用次数越来越少或完全消失的陈旧词汇。通过这种精确的语义分析，人们能够根据新技术术语的使用频率预测新兴技术。同样地，根据其术语被查询次数的减少，亦可找出日渐衰落的技术门类。其它工具，诸如美国国际商用机器公司和法国联手开发的TWatch（技术观察），则可用以大规模搜集经济情报。还有些软件可以用来搜索并分拣专利数据库——因特网上最有油水可捞的信息源。

有些程序是应客户的特殊需要而开发的。法国内务部需要一个自定义程序，它便请法国公司Language Naturel SA开发出Messie（即英语中的messiah——弥塞亚)。Messie程序的长处是进行报文路由选择，可在向法国警察局所属各部门分发信息之前对信息内容进行分析，而毋需收件人指出他们所希望在文本中看到的关键字词。根据对一个商用辞典里的诸项定义进行预先分析，Messie程序创造出了一个清除了所有语义问题的“语义网络”。

在一份公开文件中，法国国防部秘书长对几种高级信息程序的功能作了一番比较，指出“主题”软件尽管性能高得难以置信，却很难用户化；而“泰加”则要求编纂用户化的数据辞典，以覆盖软件所没有涉及的领域。国防部秘书长最后作出结论说，虽然人们在这一领域已取得一些非常实在、非常著名的成就，但百尺竿头，还得再进一步：“最需要开发的软件部分既涉及语言处理模块性能，也关系到专业领域数据辞典的编纂。要想让软件处理尽可能多的文本信息，开发这些数据辞典是至关重要的。”

哇，你的耳朵真长

经济“谍报”和经济“情报”之间，只隔一根细线。所谓情报，按照克里斯蒂安·阿尔比洛的定义，就是“搜寻和系统地判读任何人可接触的信息，目的在于了解有关意图和内容。它包含对竞争性环境进行侦察的方方面面。”

在美国，个人搜集信息的始作俑者是乔治·瓦肯胡特创立的瓦肯胡特安全公司。瓦肯胡特在90年代初期曾因给中情局和联邦政府干了点小活而一度名声大振。能源部在调查核反应堆部件的主要制造商西屋电气公司时发现，瓦肯胡特公司在西屋电气公司安装了147个电话窃听系统，其中有些系统功能十分强大，能够同时处

理多达200个单独通话。瓦肯胡特公司这种手段十分可疑。

许多公司——它们绝大多数都在美国——除经营基本的安全业务和战略咨询业务外，还专门从事高端经济情报。其中最著名也最重要的公司是克罗尔同仁公司[①]（纽约律师朱利斯·克罗尔创立），其次是富尔德公司（Fuld &Co）[②]、柯克·泰森国际公司[③]、帕沃斯公司（Parvus）和未来集团等其他几家。可以确信，在不久的将来，就会看到这个正在蓬勃兴起的市场里冒出更多的竞争者。根据靛青出版社[④]出版的秘密的《情报通讯》，在不久的将来，像库柏斯—利布兰会计公司[⑤]、德勤国际会计公司[⑥]这样的大型会计所，以及“六巨头”中的另外四家——安盛咨询公司[⑦]、安杨会计师事务所[⑧]、KPMG－皮特·马雅克会计集团公司[⑨]以及普赖斯·沃特豪斯会计事务所[⑩]，都将接踵涌入情报市场。由于这些会计所都是

---

① 网址：http：//ns.krollassociates.com/
② 网址：http：//www.fuld.com/body.html
③ 网址：http：//www.ktyson.com
④ 网址：http：//www.indigo－net.com
⑤ 网址：http：//www.colybrand.com/
⑥ 网址：http：//www.dttus.com/
⑦ 网址：http：//www.arthurandersen.com/
⑧ 网址：http：//www.ey.com
⑨ 网址：http：//www.kpmg.com
⑩ 网址：http：//www.pw.com

美国公司，因而这丝毫不能缓解发展中国家之间因日趋激烈的经济竞争所导致的紧张态势。六巨头早就控制了欧洲的财务管理，因业务之便得以搜集他们当前所服务的客户的非常特殊的资料。担心这些公司很快就会作为经济信息的猎取—搜集者来开展这方面业务的欧洲人不在少数："一些欧洲国家所担忧的乃是这一趋势隐含的战略意义，即美英可能通过六巨头更加牢固地控制全球商业情报，并打入他们至今依然鞭长莫及的地方市场。多年来，法国国家侦察中心一直都在就六巨头公司掠夺法国公司机密的危险提出警告。法国政府现在已发出各种信号，表示它准备对咨询和商业情报领域里它认为是'可靠的法国选择'的公司提供支持"。

最有名气的信息公司表示，这种业务百分之百属于"禁入区"。哈佛毕业生、克罗尔同仁公司巴黎办事处负责人让-克劳德·沙吕莫聘请前法国国家侦察中心反谍报负责人伊夫·鲍姆林为克罗尔工作。法国国家侦察中心风闻此事后，十分愤怒。他们过去的雇员为法国公司工作是一回事，但为一家外国公司干活呢？沙吕莫说，雇用前法国国家侦察中心官员是合乎情理的，是组织搜集"人才资源"信息的最佳方式。1997年1月，鲍姆林最终取沙吕莫而代之。后者因对克罗尔法国办事处的发展方向持有异议而辞职。克罗尔法国办事处刚刚开张时，所处理的信息中有百分之二十来自各界人士，另外百分之八十源于在线数据库。但他们最大一部分业务仍

然是为增进客户的利益而搜集经济信息，客户付给他们丰厚的报酬——一天3000美元。但这是值得的。朱利斯·克罗尔搜集的信息能够促成一桩生意，也能毁掉一桩生意，所以，谁在乎花这个钱呢？各种公司约请克罗尔探明其竞争对手的战略意图，有时约请克罗尔谈判在第三世界遭绑架的工作人员的赎金。克罗尔还为其它一些业绩而自豪：他曾对萨达姆·侯赛因的财产管理人进行全球追踪——据说萨达姆从伊拉克的石油收入中转移出110亿美元，用这笔钱购买的公司遍及欧洲和美国。

美国和加拿大把别的国家对美加公司的威胁当成是对其国家利益的威胁。在加拿大，加拿大安全和信息部创立了一个特别机制，专门就反谍报技术向公司提出建议，以弥补这方面的松弛懈怠状况。美国政府则通过国务院的BBS（电子布告栏系统）向企业提供资讯。公司能够通过电子形式，收到来自情报和威胁分析署的每日最新通报，其中提供了全球热点地区一览表，指明在什么地方美国人有危险，什么地方政治和经济局势动荡不安。

1992年，联邦调查局设立全国安全核查表，把潜在"威胁"——它们在最严格的意义上也对美国战略利益构不成威胁——也纳入了调查范围。在起诉位于加利福尼亚州芒廷维尤的艾米斯研究中心的过程中，就利用过这个核查表。艾米斯研究中心被控对保护头等机密信息（包括和美国国家航空和宇宙航行局所签合同的有关

文件）的重视程度没有达到联邦调查局所希望的地步。

另一关键性军事技术名单，发表于1996年。这个名单由对美国利益最至关重要的27项技术[1]组成，包罗了几乎所有技术强项。美国当局最终决定采取激烈措施反击对美国公司的侵犯行为。美国这一重大立场转变发生在苏东解体和柏林墙倒塌之后，反映出美国要避免受到新的安全威胁的明确愿望，以及同样明确的整顿现存反谍报机构，以迎接新的挑战的意愿。1994年，根据总统指示令第NSC—24号，美国创立了国家反情报政策局。这是"一个部门间组织，成员是来自联邦调查局、中情局、国家安全局、国防部以及国务院的反情报和安全专家。全美反情报中心起先负责协调国家级反情报活动，通过国家反情报政策局向国家安全委员会提出报告。[2]"全美反情报中心断言，1994年发生了446起非法经济谍报活动，危及海内外74家美国公司的经济利益。这些活动不一定非牵扯到他国政府——据各公司报告，其中仅有百分之十六是他国政府操纵的——其中大

---

① 据1996年5月，美全国反谍报中心向国会提交的年度报告，这27项技术是：高级材料和涂层、高级运输和引擎技术、航空系统、航天、军备和能源材料、生物工程技术、化学和生物系统、计算机软件和硬件、国防和军备技术、定向和动态能源系统、电子、能源研究、制导、导航和车辆控制、信息系统、信息战、制造和装配、制造工艺、航海系统、原材料、核系统、半导体、传感器和激光、签名控制、空间系统、电讯、武器效能和反措施。

② NACIC网址：http：//www.nacic.gov

多数都是竞争对手发起的工业谍报活动。全美反情报中心在 1996 年的年度报告中没有透露被指控对美国公司搞谍报的国家有哪些——这个名单是保密的。但美国政府中不肯透露姓名的消息灵通人士肯定地说，在这方面，美国的亲近盟友，如法国、南朝鲜、日本和德国，都受到怀疑。据估计，到目前为止，美国经济因经济谍报活动所蒙受的损失每月达 20 亿美元，这说明了所有狂热的报复情绪。

第九章 经济新战场

巴西政府打算重新组织一次对亚马孙地区的空中侦察，并就这一项目进行招标。15 亿美元合同的前景引起各界的广泛注意。美国主要的武器制造商雷声公司（Raytheon），以及欧洲的汤姆森公司和阿尔卡特公司（Alcatel）都参加了竞标。最终雷声公司获胜，但它的致胜之道可远不止于区区一个更具吸引力的方案——雷声公司出了新招。

美国攻势

正如美国商务部副部长 1995 年 1 月所言，巴西事件表明，现今美国政府有多么乐于帮助私营企业赢得合同和击败国际竞争对手。据说，比尔·克林顿本人也参与出谋划策，帮助雷声公司在巴西赢得价值 14 亿美元的合同。

1994 年夏季时，有迹象表明，巴西人将选择法国

汤姆森公司作这个项目，华盛顿为此天天早上八点钟就召开紧急会议。与会者包括美国进出口银行总裁、海外私人投资公司总裁、环境保护局与贸易和发展署的负责人、来自国家安全委员会、国家经济委员会以及国务院的高级官员。在这些会议上制订出如下作战方略：首先，调整美国方案，使之更接近于法国公司的方案。其次，在巴西发起反对法国人的舆论攻势，指控法国人运用贿赂手段谋取合同。协议刚刚宣布（1994 年 7 月 24 日），美国商务部长罗恩·布朗就声称，“这再一次表现出我们和美国企业并肩而立，保护美国商业利益的真诚意愿。”事实上，关于美国人如何赢得合同很快就出现了严厉的指控。而对法国人不诚实的指责从来都不曾得到过证实。在合同签署一年半之后，发觉趟入浑水、陷入窘境的正是美国自己。不过，涉及到钱，很少有好人坏人列队成行，整整齐齐站在黄线两侧的情况—— 腐败乃是一条双行道。1995 年 11 月，雷声公司在巴西被控向合同发放者行贿。阿根廷报纸刊登的窃听记录把戈麦斯·多斯·桑托斯（费尔南多·恩里克·卡罗索总统的条约负责人）和雷声公司的巴西发言人 M·阿松桑都牵扯进去。阿松桑被控向巴西参议院负责该协议的联络官吉尔伯托·米兰达行贿。这一指控在巴西内部引起政局动荡。

国际商用机器公司也陷入过类似的窘境。国际商用机器公司被控依靠营私舞弊，于 1994 年赢得了阿根廷

国家银行自动化的合约。这个合约价值2.5亿美元，是拉丁美洲国家签署过的最大的计算机合同。阿根廷总统卡洛斯·梅内姆在平息社会上对政府腐败的严厉指控后，废止了这一合同；但指定给政府高级官员的3200万美元支出也随之告吹。1996年12月16日，前经济部长多明戈·卡瓦略在布宜诺斯艾利斯举行新闻发布会，指控梅内姆总统是知道这笔支出的。

在上述两案中，贿赂行为都没有得到证实，但它们提出了一些耐人寻味的问题。正如德国非政府组织廉政与反腐败国际[1]所断言，"不同社会对待可容忍的行为，所划界限可能高低不同；但与此同时，没有任何国家的国民认为掌权者以国民最佳利益为代价，和商业承包者签订非法协议以自肥是正当的。在这样一种体制里，贿赂者和受贿者同样有罪。"

对公司来说，向合法中介人支付佣金是否非法呢?显然，如果这个中介人是属于执政党的某位政治人物，任何报酬都是可疑的。在法国人看来，这不成其为问题：只要是公开的、数目低于合同总金额百分之十五的佣金，法国财政部长都将之打入对外商务费用的预算。世界各地绝大多数大制造商都采取这种做法。在保障外国投标的正规程序之下，往往暗藏着有权有势的地头蛇所操纵的巨大的腐败网络。公款就这样被装进个人腰

① 网址：http：//www.transparency.de/links/

包，承包商对此一概宽容：他们支付贿赂，然后按与贿赂相当的数目抬高交易的总金额。

不论在商在政，美国都丝毫不想让别的国家在它的后院，或者说，就此而论，在任何与美国利益相关的地方，进行重大的军火交易。近年来，五角大楼预算削减，导致习惯于高额国防费用的武器制造商生意受到损失。毫不奇怪，信息战随之转入商业应用领域。很明显，美国政府的信息服务直接帮助了雷声公司，美国商务部长罗恩·布朗对巴西的正式访问也肯定对该公司有益无害。实际上，雷声公司总裁丹尼斯·J·皮卡德正是陪同布朗出访的代表团成员之一。这种高级别、半官方的谈判方式业已成为某种模式，美国的墨菲工业公司就是这样击败法国的巴黎机场公司，在曼谷赢得了10亿美元的建造新机场的合同。

看来，信息服务正在直接和间接地帮助私营企业洞察竞争对手的战略。有时，信息服务来得更加富于戏剧性——从旅馆房间偷窃文件；复制便携式计算机的硬盘；给电话录音和截取调制解调器传输的资讯。为了获取公司机密，他们无所不施，包括心理战。

在美国，人们围绕这个问题展开了激烈的辩论。有些人相信谍报机构应该使用他们可支配的一切手段来帮助私营企业；另外一些人则觉得，私营部门和公共部门应该像国家和教会那样彼此截然分开。

法国开始认真对待这些问题是在美国联邦调查局和

中央情报局抓住打入美国国际商用机器公司、得克萨斯仪器公司和康宁玻璃制造公司的法国特工之后。这在前面谈到过。对利用情报机构帮助企业，法国人并不受到良心的谴责。在第二次世界大战后，法国大部分制造业都被国有化。这一国有化历程相当漫长，法国人之所以如此心安理得，原因即在于此。美国人当场捉住法国特工后，新任法国国外安全总局局长克劳德·西尔伯灿前往美国相与斡旋，平息了这一纠纷。西尔伯灿解释说，随着80年代接近尾声，世界发生改变。但“美法之间过去（可能将来依旧）存在的主要区别在于，如果美国人也像法国人那么干，他们就会背叛他们对公共部门与私营部门相分离的信仰，他们就得一个劲地修正对市场经济的看法。这就是纯自由的美国社会和为达目的而兼用各种经济手段的法国的不同。”虽然前任已经确定了法国国外安全总局的发展趋势，西尔伯灿却始终反对向法国公司提供关于其竞争对手的有用情报。他相信窃取这种情报会伤害法国与盟国的关系，所冒风险太大；而且法国国外安全总局的首要工作应当是服务和保护国家。

绿色和平事件[①] 后被迫辞职的前法国国外安全总局领导人皮埃尔·拉科斯特也相信，法国谍报机构不应

---

① 1985年7月，在法国对外安全总局支持下，法国一个特别行动小组在新西兰的奥克兰港炸沉了绿色和平组织的旗舰“彩虹战士”号，法国政府起初否认与此事有任何牵连，但法国国防部长最终下台，对外安全总局局长拉科斯特被解除职务。

当冒险去帮助国内企业争取合同和打败盟国的竞争对手：“保护祖国利益的愿望不宜用来为不正当的、错误的手段辩护。如果我们谍报机构想帮助某个法国公司得到外国合同，那也不该留下把柄，要避免受到从事不道德活动的指控。”

1992年4月，美国中情局局长罗伯特·盖茨在国会讲话，陈述了他反对进行经济谍报活动的立场。但他的前任，从1977年3月至1981年1月担任中情局局长的斯坦费尔德·特纳却公开对其下属的态度表示遗憾：“为促使谍报界支持美国商业，我作了很大努力。中情局专家们却告诉我说，这和国家安全无关。”

比尔·克林顿（其前任曾是前中情局局长）对这个问题备感兴趣。看来，他很想把经济市场作为对外政策的一个方面来对待。第一次当选时，克林顿就设立了国家经济委员会，该委员会不久就开始和情报搜集部门协作，预算达180亿美元。克林顿还任命詹姆斯·伍尔西担任新的中央情报局局长。在参议院为批准这一任命而举行的听证会上，伍尔西指出，经济情报问题“在某些方面，（是）当前谍报政策中最热门的话题……这方面一大难题在于：是否在任何情况下，无论何种经济谍报，美国政府都应该和公民或公司共享。”为了进一步研究这个问题，伍尔西和国家安全顾问安东尼·莱克及白宫首席经济学家之一罗伯特·鲁宾共同准备了一份报告。

中情局局长伍尔西因艾米斯间谍案于1994年12月

29日辞职。离任之际，他对中情局新工作重点的几个方面作了说明："我们不为私营公司当间谍，但这的确意味着我们会把外国这些腐败行为通报给白宫、国务院和商业部，引起他们注意并随即寻找通常都会奏效的补救办法。"当然，要有力打击在商业领域玩弄肮脏把戏的公司和国家，就需要知道主要玩主的情况及其所作所为——生产、研究、现金流动、销售网络、中间人。所有这些很像老式谍报活动搞的那一套。伍尔西的新立场没有被忽视，因为—— 他说的不正是许多人想听到的吗？正如一位前中情局特工对《华尔街日报》所说的那样，"历史上，政府和企业之间彼此仇视，许多企业主管人员不想沾染上与间谍有关的污点。可能这就是为什么美国电话电报公司（AT&T）说：'这种事情我们不需要中情局的帮忙，非常感谢。'"

1995年7月14日，比尔·克林顿正式宣布美国立场的重大变化。在弗吉尼亚州兰利中情局总部，克林顿总统面对中情局官员，再次明确表示他无意拆散中情局，因为他不相信"身体好就可以取消健康保险。"在承认冷战结束的同时，他强调，新的威胁来自经济方面，对此美国要作好准备。他说："少数人呼吁我们放弃中央情报部门，我认为这些观点大错特错……是的，我们的国家安享和平，我们的经济不断增长。在世界各地，民主和自由市场正在前进。但所有这些进展，没有一样是不可避免或不可逆转的。对人类心理或人类精神活动的

每一项研究、每一本宗教小册子都告诉我们，世界上总会有各种各样的麻烦、战争，以及关于战争的流言，直到时间终结。”

克林顿继续谈到中情局在经济和工业谍报方面发挥的积极作用，坦率指出这些行动具有重要意义。他强调，这只是用来帮助诚实的美国公司对付挡住他们成功之道的不诚实的竞争者。克林顿热情称赞那些帮助“揭露骗取美国公司亿万美元的贿赂行为（的人）……你们的工作促进了美国的繁荣。”

《洛杉矶时报》记者詹姆斯·莱森说，在经济新战场上，美国情报部门的投入程度，令白宫经济学家“为中情局成功地适应新的工业和经济任务而深感愉悦。官员们从中情局在经济谍报中的适当作用的内部争论中得出结论说，这类反谍报活动是中情局能够而且应该发挥作用的一个领域。中情局官员相信，他们不应代表美国公司直接从事针对外国公司的谍报活动，而且应当将其隐蔽的经济谍报活动限制在诸如贸易谈判、保护美国公司免遭外国特工渗透、以及在发展中国家或其它地方，揭露妨碍美国公司竞争的、牵涉到外国企业或官员的贿赂和腐败行为。”

事实上，在经济谍报领域，中情局的成功不仅仅限于在巴西帮助了雷声公司。美国情报官员私下里同意并且承认，许多美国公司都一直控制着政府的信息谍报工作，尤其是汽车工业。“但是，这群小偷不是邻区的匪

帮，也不是有组织的犯罪团伙成员。你持有文件证明你买下了汽车，而且每月向银行付款。同理，银行也将出示它从福特、通用汽车公司或克莱斯勒购买的收款资格。尽管如此，这三大美国汽车巨头将是被盗物品的受益者，作恶的人则仍然是中央情报局里搞见不得人的谍报活动的专家。”据报道，1995 年上半年，美日就汽车进出口展开紧张谈判之际，美国特工就向美国谈判代表提供了情报。而且这种众所周知的帮助，对当时的美国首席谈判代表米基·坎特来说，既不是头一回得到，也不是最后一回。

1993 年和 1994 年欧美关贸总协定谈判期间，法国立场强硬，引起美国国家安全局对法国政府的密切注意。法国内阁部长们都有个图方便（或者令人恼火，看你从哪个角度看）的习惯——好从飞机上给办公室打电话。在最敏感的最后谈判阶段，他们的交谈很容易被窃听，而且毫无加密系统保护。干这种事对美国国家安全局来说完全是小菜一碟。法国在沙特阿拉伯就 300 多亿美元的飞机销售合同谈判时也出现过类似的麻木不仁的情况：当时的法国总理爱德华·巴拉迪尔在没有防护措施的跑道上，说出欧洲人的最后打算，害得空中客车公司输给了波音和麦道。不过，可能有人会争辩说，由于美国一直对谈判施加政治压力，法国早就败局已定。比尔·克林顿在和沙特阿拉伯国王法赫德会谈时，就曾几度亲自过问此事。

美国人并未独霸通讯谍报之天下。法国人及法国国外安全总局也擅长利用这种技术。1994 年，图西族领导人保罗·卡加梅统治卢旺达之后，法国人窃听了卡加梅的电话，而且收获不小。法国总统弗朗科斯·密特朗据此于 1994 年夏季在联合国支持下对卢旺达发起绿松石行动。美国曾赠送这个叛乱头子一台和国际海事卫星组织联网的移动式卫星电话，事实证明它对法国人完全“透明”。美国人一经发觉卡加梅的通讯遭到窃听，很快就向他提供了更高级的设备①。

中情局特工在巴黎

1995 年上半年，美法因为国际合同的竞争，关系高度紧张。法国内政部长夏尔·帕卡将一批美国中情局间谍从法国驱逐出境。这一行动背后的政治动机很明显，就是要帮助总理爱德华·巴拉迪尔竞选总统。但由于报界对中情局特工的违法行径作了广泛深入的报道，使得这一事件格外引人注目。从官方立场上讲，友好国家被认为是不会在对方国家刺探情报的。但这次事件之所以异乎寻常，不是因为中情局在法国从事间谍活动，而是因为他们被抓住了！而且，过去在盟国之间也发生

---

① 在 1994 年卢旺达胡图族人屠杀图西族人之前，法国支持那里的胡图族人，而美国支持图西族人。

过类似的事，但公开报道驱逐事件却一直十分罕见。

美法之间出现一些重大纷争并没有伤害两国关系，它们为主要事件作了背景铺垫，许多争端在80年代法国国外安全总局打入美国公司（如国际商用机器公司）时就已经解决了。当然，虽然克劳德·西尔伯灿当时出色地抹平了美法之间的裂痕，法国人还是在美国落了个骗子的名声。这期间，受到中情局监视的法国外交官之一——法国驻休斯顿总领事伯纳德·吉耶——调任内政部长夏尔·帕卡的外交顾问，协助处理全部有关中情局的事务，但也无济于事。

一段时期里，美国调整其全球情报工作方式，在商界搜集情报。这期间，在美国从事经济谍报活动，既惹人注意，风险又大。美国相信，经济谍报关系到许多美国公司的生死存亡。在航天、武器、电讯和农业领域清除竞争者，成为头等大事。为达此目的，有关情报来自私营还是公共部门倒无关紧要。美国特工打入巴黎的企图没有得逞——虽然他们没一人当真被驱逐出境——这在华盛顿看来是灾难性的。在参议院授命下，中情局总检查长弗雷德里克·P·希茨领衔展开调查，一时间指控满天飞。1995年5月，约翰·多伊奇主持中情局后，第一件事就是惩处欧洲部负责人约瑟夫·德·特拉尼，不准他到巴黎接替迪克·荷尔默，后者曾负责修补潜入法国政府的行动的烂摊子。

信息搜集和分析问题向各公司提出了挑战。对此，

各公司虽有进展，但仍感困难。这一领域的一流专家菲力浦·包马德这样谈到这个问题：“各机构缺乏时间来理解它们的处境。信息从四面八方涌来，令公司之舟淹没在成吨成吨的紧急需要、最新特别报告、不断累积的24小时在线新闻等等之中……不妨把公司看作是一个翻译系统，其中浏览、翻译和领会是密切相关的二元关系。浏览处于公司与所在环境之间关系的核心位置，因而也是理解公司的关键，公司不是在信息汪洋中航行，信息要在明确的翻译系统里搜集和孵化。”

许多私营信息公司因此应运而生，生意兴隆。为搞到私营企业关心的信息，他们用上了谍报机构所有的基本策略和手段，并作为大公司的转包商开展业务。法国的 Inforama 国际公司虽然几乎不为外界所知，在经济信息搜集方面却是世界级大腕。该公司是前炮兵军官和谍报机构的高科技专家罗伯特·吉约莫创立的联合大企业 Inforama 的子公司。Inforama 在亚洲各地的业务增长十分迅速，在美国另设有一家专门开发软件、电讯和计算机技术的子公司，名叫高科技咨询集团。Inforama 雇有225名工程师和管理人员，一方面协同开发软件，另一方面在全球各地设立信息搜集处。他们的软件内容从电子战模拟仿真到间谍飞机和间谍卫星图像的解读程序无所不包。法国政府也使用他们的软件，光顾他们信息搜集处的客户都是顶尖的法国公司，因而其业务成果十分可观。毫不奇怪的是，在 Inforama，人人对公司业绩含

糊其辞。谨慎是该公司的指路明灯。

职业俱乐部和公开信息源

Inforama 的创立人对竞争性情报业者协会[①]情有独钟，以致成立了法国分会，对此没有人感到意外。竞争性情报业者协会对独立的经济信息搜集者来说，是一个聚会聊天的社交场所。协会成员都是具有相似意向或目的并从事类似工作的人，协会为他们提供了宽松友好的交流思想的环境。竞争性情报业者协会于 1986 年由费伊·布里尔在美国创建，现由太平洋贝尔信息服务部的特蕾西·斯科特领导，大约有三千名成员，每年举办一次年会。会员赞同瑞典经济信息学家斯特万·德迪耶尔率先提出的“信息公开”主张，讨论《竞争性情报评论》以及和他们工作有关的道德问题。在他们看来，竞争性信息——即搜集和分析商业竞争对手的情况——只能在规范化的环境里方可进行。他们在网址上陈述了自己的信条：“为提高本行业尊严和社会认可而不懈奋斗，勤奋热情地履行职责，同时保持最高度的职业感，避免一切不道德行为。忠实地坚持和遵守所在公司政策、目标和方针，遵守所有有关法律，在所有访谈开始前，准确透露所有相关信息，包括个人身份及机构。充分尊重

---

① 网址：http：//www.scip.org

所有对信息保密的要求。在公司和第三方订约人，以及在整个行业内，提倡和鼓励完全遵守这些道德标准。”

国家情报机构和搜集经济情报的公司之间存在很大不同，不仅运作规模大小有别，而且所使用手段差异也非常大。从理论上说（大多数情况下都是符合实际的），私营公司回避非法手段，而谍报机构靠非法手段吃饭。谍报机构游走在法律和政府边缘，通常都设法阻挠团体、个人或政府采取非法或法律体制难以控制的行动。当然，谍报机构自己则使用古往今来所有手段大胆地、非法地搜集经济信息。

私营信息公司的活动范围依旧局限在“公开”信息的天地里。多亏高级信息领域的最新方法，他们从可利用文献（绝大多数时候是通过电子手段获得）中发掘出大量信息。一些专家说，他们想要的信息百分之九十五都可以通过这种形式得到，余下百分之五则是政府谍报机构要设法探听的。在这方面领导世界潮流的专家之一是罗伯特·斯蒂勒，他一直在为完全公开的情报源奔走游说，并自己创办了开放源解决办法公司。1993 年 7 月，他在向中情局提交的备忘录中表述了公开情报源（OSCINT）的概念。他说：“今日情报所必须涉及的威胁范畴发生了剧烈的变化，我的重点即在于此。公开情报源在效果方面，既能让分析人员满意，也能让消费者满意。从更广泛的层面上说，情报能够增强我们的国家安全和民族竞争力。公开情报源作为更大的国家‘信息

连续统一体’的一部分，可以充分用来满足消费者的需要……当前，美国情报史正处于一个特定时刻，需要有见识、有个性、肯冒险、思想开放的领导人，对美国情报事业进行彻底改造和重新利用。”斯蒂勒相信，借助这样一种安排，围绕公开情报源观念重铸完全美国式的信息搜集体系，所有各种各样的问题都将迎刃而解。

认真说来，在中情局眼里，斯蒂勒是个喜好破除旧习、标新立异的人物。他曾是中情局南美行动的负责人，后来加入美国海军陆战队重建海军陆战队情报中心。现在，斯蒂勒又全身心投入私营企业，尽一切努力要让周围人转而接受他的世界观。尽管中情局和斯蒂勒关系时断时续，斯蒂勒看来还是获得了成功——中情局新近设立一个职位，由保罗·F·沃纳支配，专门研究公开情报源。沃纳在 1993 年 10 月出席过开放源解决办法（OSS）第二届全会。

斯蒂勒甚至还到法国寻找信徒。他主要在法国国外安全总局和军事情报指挥中心引起了一些积极的反响，但法国内政部长却老大不高兴。一些人认为，不管斯蒂勒在公开场合怎么谈论从前的中情局老板，他的经历使人很难信任他。在法国，谋取这种“公开信息”是违法的[1]。因此，当开放源解决办法公司试图就开放源和信

[1] 法国刑法典禁止为别国利益搜集“公开信息”，这有点奇怪，但事实如此。

息高速公路课题在巴黎举行会议时，法国当局要他们别打这个主意。

日本人：信息经济大师

在经济情报搜集领域，日本幽灵越来越显得突出。在这方面，大多数专家，包括德国阿托歇姆有限公司经济情报网主任弗朗科斯·迦科拜克在内，都说日本之所以取得如此令人震惊的成就，原因在于它的高超技术。日本“一直专心致志地、谨慎地、系统地梳理全球存储的公开发表的各种信息，尤其是有关主要工业化国家的数据。对信息的细心留意和审慎使用使日本取得令人眩目的成功。如果说美国、法国、德国和英国的大公司难以看到合作的必要性，如果说它们当中一些负责人还指望从政府那里得到再多一点帮助，这种事情是不会发生在日出帝国的。如果日本人的成功首先靠的是模仿我们，然后再自行创造，为什么我们现在就不应该模仿他们呢？

在日本，很少有人不同意这个说法：搜集对私营企业有好处的信息，乃是他们成功的必由之路。日本首相办公室专门下设一个机构，负责政府信息机构和私营企业之间的沟通。熟捻日本经济复杂情况的法国专家克里斯蒂安·哈布洛特说，私企经理和政府信息机构之间的关系非常特殊，不受一般法规限制。“时至今日，日本

搜集信息的能力在深度和速度上都已成为世界榜样。其它国家的数据库相形见绌，而且毫无迹象表明它们能在可预见的将来赶上日本。日本人早已处在这么一个位置，它可以驱使世界各国来到谈判桌前，向它们提供访问全球性信息网的渠道，而这一全球性信息网，将由日本加以控制。通过确保信息流动和对其进行战略性的内容管制，日本正在改变经济战的规则，使之符合自身利益。”

日本虽然在大踏步向前迈进，但总的说来，它对因特网或数据传输网络还不适应。日本业已帮助许多亚洲国家配备了以这样或那样的方式连接其网络分析工具（搜索引擎等等）的高速度数据线，日本也确实预见到了信息高速公路的巨大发展，包括在20年之内，每栋住宅里都接通光缆。尽管这些进展内容具体且有条不紊，日本人却对使用网络进行个人通讯不感兴趣。大力倡导日本发展因特网的石田治久解释说，教育部官员主要关心的是他们停止控制连接全球网络的服务器。石田说，这些教育部官员甚至没有兴趣试着了解因特网，了解因特网为何这样受欢迎。“甚至我们向他们解释的时候，他们还是不懂。”

尼古拉斯·内格罗蓬特是美国麻省理工学院媒体实验室骨干，叱咤网络空间的领袖之一。如他所言，正是日本开发出风行世界的通讯技术——传真机。“传真是日本人的传家宝，但这不只是因为日本人伶俐到比其他

任何人都能更好地、标准化地生产传真机。这是因为日本的文化、语言及商业习俗都在很大程度上以图形为主导…… 日本汉字的象形本质使得传真机的出现顺理成章。因为当时几乎没有什么日本人采用计算机可读形式，也就几乎没有什么不便。另一方面，对一门和英语一样符号化的语言，就计算机可读性而言，传真机无异于一场灾祸。”

日本不情愿适应信息时代，招致普林斯顿大学肯特·E·卡尔德等学者的抨击。他们指斥日本的明显缺陷，发出古希腊女预言家卡桑德拉式的不祥预言："在这个新世界，许多古老的、长期被吹捧为日本力量所在的地方行为和组织形式，包括日本传统上对大型集体项目与不加选择的行政干预的偏爱，现在看来都渐渐趋于过时了……就一个技术先进的国家而言，日本在开发因特网服务方面也依旧有名得慢。事实是，排名世界第二的日本经济现在所拥有的主机不到全球因特网主机的百分之五，而美国则将近三分之二……现在是日本认真思考在国际合作中，如何增强自己作为国际商务中心的吸引力的时候了。尽管日本经济规模大，国民勤奋，但却越来越偏离信息时代的竞争主流。要避免令日本有落伍危险的这种‘回避现象’，关键在于变革。[1]”普遍认为，日

---

① 卡尔德：《日本有被信息时代绕过的危险》，《亚洲时代》，1996年11月8日。参见网址：http：//www.asiatimes.com

本人对这些观点并未装聋作哑，但也没有能力迅速作出反应。

日本人厌恶因特网的情绪大约持续到 1995 年，但随后就非常引人注目地消失了，取而代之的是强烈的热情。因特网倡导者从启发教育入手，向大众宣传网络在日常生活中的积极作用："在传统上，日本人把政府和官僚机构当成'上级'，把公共安全和福利任务托付给他们。每当事情发展不遂所愿，就容易抱怨。不管怎样，'公众'必须由自行其是的'个人'来加以维系，这称为'自治'。如果他们一味这样把任务指派给各级官员，而自身毫无主动性，他们最后就会自己窒息自己。"1996 年，因特网在日本各地爆炸式地流行起来。日本一度远远落后于美国和斯堪的纳维亚半岛，现在则一直在弥补失去的时间，突飞猛进地向前发展。1996 年 6 月，数据集团公司出版第一本《必用信息索引》，按参与信息社会的能力把各国分出等级。从最低到最高，为"慢跑者"（中国、土耳其、沙特阿拉伯）、"赛跑选手"（俄罗斯、智利、爱尔兰）、"大踏步前进者"（英格兰、加拿大、澳大利亚、以色列、日本）、"溜冰者"（美国、瑞典）。"大踏步前进者"的特点是"谨慎、坚定、连贯、有目的、成功的长期因特网投资"。实际上，日本在以光速前进。电讯巨人日本电报电话公司（NTT）已创建开放计算机网络，希望由此连接大多数日本网上冲浪者。1996 年一年里，日本因特网订户从

150万上升到850万，真正是爆炸式增长。

过去，日本人明显讨厌因特网，这和关不关心进步过程显然无关。相反，日本人受到技术进步观念的推动，公司利用网络搞信息和侦察的专业水平不亚于美国和欧洲同行。有的公司对通过因特网向遥远的数据库渗透也有同样的兴趣。日本首相自己设有处于萌芽状态中的情报机构，名叫日本科学和技术信息中心。在日本，考虑到和其他发达国家的情报机构铢两悉称，这类组织中最重要的当数日本外贸组织（JETRO）。全球共有80个日本外贸组织分部，每个分部都负责搜集所有有效信息，对任何显然难以获得的信息也穷追不舍，直到最后弄到手为止。以同样的方式，Sogo Sochas之类著名组织——尽管它们甚至更紧密地融入了其他国家的经济之中——也在全球雇用了6万多名职员，搜集他们所能找到的一切。在每个大城市（在巴黎、纽约和华盛顿特区均超过1,000人），他们的特工都数以百计。这些特工打进各种集团或某些特殊企业（野村、三菱、大和），工作在所有想象得到的部门，游荡在具体或虚拟的专业人员出没之地，每天都向日本总部发送报告。依靠这些建制，日本人对绝大多数市场变化的反应比所有人都快，他们有能力预期法律变动，更新产品，使之超过老标准。在其他人还在迎头赶上的时候，他们就搞定了新产品。日本人比任何人都更会钻欧洲法律的漏洞，结果他们卖出的汽车、摩托车、电器和家庭用品比所有竞争者

都多。

作为90年代初的因特网先驱，美国公司的各种日本分公司在经过和日本政府的艰难谈判后，都设法连上了因特网。主要网络日本创始因特网（Internet Initiative Japan）在一段时间里，仍然是处于被软禁的状态，听任想上网的人们在各大学间进行缓慢、原始和透明的联络。直到前不久，由于Bekkoame（自1994年9月起提供上网服务）等公司的努力，普通的日本人才开始能够上网。但是，日本经济企划厅[①]创办日本经济万维网的一纸命令，与其说是新时代曙光初露端倪，不如说对日本媒体更有意义。日本观察家说："因特网复苏了权力之争……这一危机暴露了日本技术热的局限性，也表明日本无力理解现代政治的基本原理，特别是国民乃民主之本的原则。"

早在因特网海啸吞没日本之前，许多企业就已针对职业用户和信息买主——他们有充分的理由要长期使用网络——的需要，设计和实施了适应信息社会的战略。继"计算机在线新闻服务"（Comline News Service）[②]之后，日本很快就推出了庞大的收费在线信息数据库。这个数据库可通过三菱研究所的Dialine－Ⅱ链接，并提供技术和商业信息。法国的日本问题专家克里斯蒂安·哈

① 参见网址：http：//epa.go.jp

② 网址：http：//www.twics.com/COMLINE/database.html.

布洛特指出："为了成为世界首要的科技信息来源，日本人首先开发自己的信息，将它们经过慎重筛选和考虑后翻译成外文，利用语言障碍获得优势。现在他们可以迈向超级信息阶段，出售业经试验和完成的信息产品。日本企业家把经济情报置于更突出的位置，从而把集体信息文化、实时数据管理、以及公司战略模式整合在一起。"

日本人也能够实现这一目标。到 1994 年年底，3，000 多个遍及日本、包罗万象的数据库中，只有 353 个可以从国外链接使用。而日本数据库促进中心提供的最新统计资料表明，使用次数最多的数据库是：科学文献库 JOIS—JICST、证明、许可证和文凭库 PATOLISJAPIO、公司和企业数据库 COSCOS2（TeikokuDtanank）、金融数据库 TSR—BIGS、法律库 TKC、炸鸡库 KFC 以及股票市场数据库 QUICK。显而易见，日本人地位之优越，大有主宰新的信息市场之势。数据库促进中心宣传主任启介在该中心网址上谈到其服务系统时，表现出某种可疑的直率。他说："海外需要日本信息不断增加，而日本现在有责任推动日本信息的国际传播。[①]"

① 启介：《日本数据库概况》，参见网址：http：//www.dpc.or.jp/

第十章 盛世危言

1994年2月4日发生了一件事，其本身微不足道，但却有着重大的象征意义。这一天，美国总统比尔·克林顿和瑞典首相卡尔·比尔特交换了电子邮件。比尔特在电子邮件中感谢克林顿取消了自1975年起生效的对越南贸易禁令。比尔特最大限度地利用这个机会写道：美国和瑞典看来很适合成为最早利用因特网充当外交和通讯手段的国家。克林顿用预言家的口气回答说，他和比尔特首相一样，对这种新技术的前途和潜力深具热情。克林顿就任总统仅仅一年，就从个人电子信箱里收到了十万多封电子邮件[①]。不过，任何稍微重要一点的外交信函，基本上都不会通过因特网传递——在当时，超出象征意义，因特网就实在太不可靠。

---

① 美国总统电子邮件地址：president@white-house.gov 白宫网址：http：//www.whitehouse.gov

进还是退?

通常,“信息战”被认为是国家或公司之间的冲突,其定义即:国家或公司使用多种手段在网络空间进行竞争或战斗。也有其它战场。在世界各地,富国和穷国、富人与穷人之间的冲突早已以各种各样的形式在进行。

在遥远的过去,有没有一部电话、一辆汽车、一台电视、或一个室内抽水马桶就标志着富人与穷人之间社会地位的天差地别。现在,上网成为地位的象征。虽然如此,但不管有没有钱,受过大学教育的人作为一个群体,在工作场所或家中没有个人计算机的是极少的,而且其中至少一半个人计算机都带有调制解调器。对在校大学生而言,不用计算机几乎没法想象。他们的计算机要么是自己的,要么由校方提供。对科学家、学者或商人来说,不用计算机工作也已经几乎是不可能的事情了。

1994年,美国人在计算机设备上花了80亿美元,几乎等于每年花在新电视上的钱。比什么都有力的一个数字是:百分之三十的美国家庭都拥有计算机。它们没有全都接收在线服务,但因特网概念正在普及,正在被谈论、使用,越来越打破常规。因特网的优势如此昭昭在目,以致出现了一种“网络民主”,可令普通公民越过政治家们排得过满的世纪末日程表所造成的障碍,直

接和他们接触。电子邮件不会打扰会议，也不会让收件人淹没在成吨的传真纸里。尤其是特殊利益集团，早已利用电子邮件递交他们的请愿书，国会议员也用电子邮件和选民联系。商业服务商，诸如吉尼联机公司（GEnie)、计算机服务公司、天才联机公司以及美国在线都向消费者提供政治家网址链接的特别服务，而政治家们对这种直接访问也全都趋之若鹜：允许选民与他们办公室直接链接而且实际免费。这样，政治家们就可以把时间和金钱花在别的事情上，而不是他们惯于依赖的电视广告节目。有的政治家甚至还有自己的服务器，方便投票者就某个特别主题或有待解决的问题访问有关站点，或前往站点浏览他们的代表就当天重要问题所作的最新意见书。

皮埃尔·列维对这个问题持乐观看法。他不认为现行投票体制会直接转换到虚拟的电子领域——国会或总统选举不会采用电子邮件形式进行。列维注意到，一场改革正在进行之中，他当即着手研究网络技术对真正的直接民主的出现将会产生多大的影响。列维相信网络空间里存在这样一种机制，它“……将让每个人都可以持续地帮助开发和提炼共同关心的问题，提出新疑问，展开新辩论，并就形形色色的议题阐明独立的见解。公民们将共同精心构筑起五颜六色的政治景观，而不会预先受到不同党派的阻隔遏制。公民的政治身份取决于他们对建设变幻无穷的政治景观的贡献和对各种问题的支持

（最重要）、（他们将坚持的）立场、以及（他们将依次利用的）论据。这样，每个人都将拥有完全个人化的身份和角色，截然不同于其他人等，同时得到和其他在给定政府的给定主题上有类似或互补观点的人共同工作的机会。显然，需要有些手段来保护政治身份的隐匿性。我们不再是通过给某个政党添点分量或者协商某位发言人的合法性，从而作为'大众'来参与政治生活；而是通过创造多元化的、充满活力的集体思想，对共同关心的问题的确立和解决作出贡献。"只要确信这种新技术工具不会使普通人疏离新通讯手段，人们就会趋于同意列维的观点——个人计算机的复杂性，多半就像上个时代电视、电话和汽车最初出现时那样，将被战胜。个人计算机将成为我们日常生活中的有机组成部分。

"个人报纸"是网民不得不掌握的又一项服务。《夏洛特观察家报》、《今日美国》、《芝加哥论坛报》、《阿尔伯克基论坛报》以及《圣路易邮报》都已经上网相当一段时间。《华尔街日报》[1] 有自己的服务器，《纽约时报》[2] 可以通过美国在线和万维网看到，《华盛顿邮报》[3]在网上有非常优秀的免费互动编辑。网上还能看

---

① 网址：http：//www.wsj.com/ 一年50美元，即可订阅该报用户化的电子互动版。

② 网址：http：//www.nytimes.com，《纽约时报》的电子版订阅费相当昂贵，每月35美元。该网址非用户无法人内。

③ 网址：http：//washingtonpost.com/

到《洛杉矶时报》[1]，该报并以每篇文章1.5美元的价格开放其在线档案库。每个月都有大量新报纸和杂志出现在因特网上，以致没有网址的报刊很快就成了漏网之鱼。在欧洲，伦敦的《每日电讯报》可以以《电子电讯报》的虚拟形式看到，法国和欧洲大陆其它地方的报纸迅速群起效尤，发布了国家级报纸的电子版。法国全国性大报之一《解放报》[2]有自己的站点，全球在线向订户提供各种报纸以供选择。法国日报《世界报》[3]也有自己的站点。1996年，成千上万的其它出版物也上了网。出自洛桑的瑞士站点 L' Hebdo 对全球五花八门的媒体网址作了精彩"展示"[4]，为有兴趣者所必备的工具。还有只在网上发行的报纸，如 Pointcast 和由微软和美国国家广播公司电视台联合创办的 MS—NBC[5]。这场通向因特网的渐进的革命，以清晰的经济和编辑战略为基础，引发了一些严重的问题。

不会使用计算机的人们怎样才能在这个日益依赖技术的社会生活呢？文盲如何能够进行电子通讯？人们怎样才能既不必花一大笔钱购买基本设备，又可以获得必

---

① 网址：http://www.latimes.com/

② 网址：http://www.netfrance.com/Libe/

③ 网址：http://www.lwmonde.fr/

④ 网址：http://www.webdo.ch/webactu/webactu-presse.html/

⑤ Pointcast：http://www.pointcast.com/；MS - NBC：http://www.msnbc.com/news/default.asp/

需的专业技术来掌握这些工具?

美国相当重视这个问题。商务部长罗恩·布朗问道:“怎样创造环境,才能使得我们有朝一日建成信息基本设施的时候,社会界线不会变得泾渭分明?”现在,懂计算机的技术工人的报酬,已经比技术水平相仿,但不懂计算机的技术工人的报酬多出了百分之十五。在美国中小学,有没有计算机,差别越来越大。一些学生课堂里配备了强大的计算机和因特网链接,老师能够把因特网和网上冲浪揉合到教学过程之中。而在另一些学校,如果所有学生都有课本就算幸运了。巴巴拉·坎特罗维茨在 1994 年 3 月 21 日的《新闻周刊》上著文指出:“对不那么运气的学生,信息高速公路就和通向奥兹(电影《绿野仙踪》中的仙境——译者)的黄砖路那么虚无缥缈。”

因特网不仅远不能带来新一轮教育民主化,而且可能会大大强化贫富之间、局内人与局外人之间、受到良好教育的人与文盲之间的矛盾。许多人都趋向于这个观点,预言有朝一日,信息时代泰坦尼克号可能会撞上潜伏在历史水面下的冰山。学者马赫迪·埃尔曼加拉认为:“人们在采纳日新月异的信息技术的同时,必须同样地警觉到信息技术的进步对社会的强烈冲击;尤其应该注意到科技文盲的增加。这只能使信息技术的益处受到局限,甚至有可能左右我们的民主政治体制。社会需要开展新的行动,以促进知识设施的开发,从而吸收信息技

术演变所带来的根本性变化。”

内战？

贫富之战会发展到网络空间吗？如果这种可能性在所谓发达国家早已是活生生的现实，那么，只有假设这种动态很快就会出现在第三世界，才算把这个问题说全面。比如说，在尼日尔、危地马拉和柬埔寨，现有电话系统就不像在欧洲、美国和日本那么先进和完善。通讯网络的全球化只是一个特定的主观概念，因为地球上还有太多地方没能包括进去。某些国家（如印度或印度尼西亚）业已吸引了一些计算机转包项目，它们主要从事编程和数据收集工作，通过电子网络传送给不过问业务的合伙人。在印度尼西亚，这类信息收集工作大多还非常初级，比如复制电话簿那样庞大冗长的文本。但印度操作员的教育水准高得多，能够进行非常尖端的信息分拣和软件开发，比起在欧美做的费用，要省下很大一笔钱（印度操作员平均一年只挣 3,000 美元）[1]。但这只不过是廉价劳动力在高科技领域的新应用而已（这些工作在发达国家做不了，因为人工费用太高），并没有出现实质性的进步。城市学家和哲学家保罗·维瑞利奥指出：“电讯发展使得低附加值服务业（如日常管理活动和货

---

[1] 参见网址：www.ina.fr/CP/MondePiplo/

物发运）受到较穷国家的竞争。富裕国家在信息高速公路上正以非常危险的速度疾驰，它们试图也让没那么富有的竞争者们放开步子……”

保罗·维瑞利奥一生都在研究策略和战争的速度。在他眼里，信息以虚拟形式进行“即时直接交换”预示着工商业将要出现严酷局面，是政治和社会两方面新的不平等的潜在来源。他说：“今天，暴政正在登上虚拟论坛。个人即时交换电子信息的能力有多么了不起，所有这些互动行为的负面就有多可怕。我是国际主义者，我的父亲是移民，我不打算拿民族主义当盾牌。我同意能够相互尊重边界和文化差别的世界公民的概念，但我怀疑有地球统一、人类大团结的至高无上的那么个时刻。在我看来，统一需要暴政，而且网络空间正在朝着这种暴政，而不是虚拟现实的磁头组的方向发展。危险很大，我们必须奋起战斗，因为这种渐进的发展不一定是无法避免的。”

这个问题并不见得像这些观点表述的那样已成定局。就算真正的全球接触信息网络对发展中国家还是遥远的现实，这种技术也有其非常积极的一面。首先，现有网络可以帮助这些发展中国家把上网的麻烦减少到最低程度。加利福尼亚的“和平网”（Peacenet）组织就向全球数以百计的活动分子团体提供了上网渠道，帮助它们争取教育和人权。和平网是进步通讯协会（APC）网络的

一部分，后者还包括“生态网”[1]（Econet）（又称“依可网”，专门解答环境问题，并提供和英国生态网“绿网”（Greenet）的链接）、“纠纷网”[2]（Conflictnet，以仲裁问题为中心）、“劳工网”（Labornet，专谈社会改革）、以及“妇女网”（WomanNet，以女权主义问题为中心）。网络在世界各地蓬勃兴起：印度有“第三世界网”（Third World Net），澳大利亚有“飞马网”（Pegasus），墨西哥有 Laneta，南非有 Sangonet，举不胜举。

因特网甚至使孤零零的俄罗斯城镇可以通过 Glasnet 网[3] 和世界相连，否则这些城镇就完全与世隔绝。1993 年 10 月，俄罗斯工会会员亚历山大·谢加尔、鲍里斯·卡加里特斯基和弗拉基米尔·康德拉托夫被警察拘留，全靠 Glasnet 帮助才获得释放。莫斯科主要的工会总部首先向全世界的工会成员及友人发出电子邮件，告诉他们拘押工会会员的警察局的电话号码。一下子，这个警察局就完全埋没在来自美国、日本和欧洲的电话雪崩里，受到全世界的压力。拘捕者屈服了，让这些工会会员开路。这个故事我们虽然是辗转听来的，但它加深了这样一个观念，即因特网不仅传载报纸、滋养间谍和繁殖资本主义，它还能有更多的功能。

---

① 网址：http：//www.econet.apc.org/econet/

② 网址：http：//www.igc.apc.org/conflictnet/

③ 网址：http：//www.glasnet.ru/brochure.html.

在非洲，只有寥寥几所大学连上了因特网，而且它们只是用因特网来收发电子邮件。在南非、埃及、突尼斯和赞比亚，因特网都在发挥作用。在肯尼亚内罗毕出版的电子报纸《非洲经济新闻》通过一个乌拉圭网络（NGOnet，是一个总部设在乌拉圭首都蒙得维的亚的非政府组织网）进入因特网，追踪非洲网上冲浪者沉浮盛衰的最新消息。该报曾载文说："经常航行在网络空间的非洲因特网用户乐观地认为，由于不懈努力，过去阻挠上网的政策可能会发生变化，从而使非洲绝大部分地方能够在未来一到两年内，都连上因特网……当然，在非洲使用因特网技术还存在没完没了的问题——繁忙的电话线、调制解调器故障、丢失信息、负责解决技术困难的系统操作员工作负荷过重，收入过低，而且这类人材还极为匮乏。[①]"

荒谬的是，要改善非洲电话线路短缺问题，恐怕需要利用许多国际大财团正准备投入使用的不同凡响的新卫星电话网络。有 12 家不同企业都正在开发卫星电话网络，争先恐后要分得一杯虚拟之羹。它们的想法是让人们用上无需地面中继而直接连通卫星的小巧的手提电话，而且希望这种卫星电话网能够取代现存的业已开通的移动电话网。你可以想象一下，如果所有硬件都安装在太空，这种系统的费用就可能低很多很多。铱星是这

① 参见网址：http：//www.web.apc.org/econews/

种系统中最先进的，它将于1998年9月起投入运营，并将发射66颗卫星进入近地太空轨道。这个项目耗资50亿美元，牵头的摩托罗拉公司拥有四分之一股份，其他投资者包括斯普林特公司、雷声、麦克唐奈－道格拉斯航空设备制造公司、洛克希德、意大利都灵电话服务公司和德国的Verbacom公司。第一颗铱星卫星已于1997年5月从加利福尼亚的范登堡发射上天[①]。另一个进展迅速的项目是全球星（Globalstar），它是劳拉公司和Qualcom公司的产儿，得到阿尔卡特公司和法国电信公司的大力资助。全球星将使用48颗卫星，耗资17亿美元。在远地轨道，Odissey公司和Oco公司雄心勃勃地想创建“仅仅”包含10颗卫星的网络。比尔·盖茨的微软公司则正在策划一个90亿美元的项目，想要发射840颗（！）与地球的相对位置不变的近地轨道卫星——这笔费用很成问题；而且这么多颗卫星构成的系统显然必定十分复杂。1997年3月，法国也加入竞争，阿尔卡特公司投资35亿美元进行“空桥”项目，要发射60颗与地球的相对位置不变的轨道卫星。无疑，大公司的竞争可以保证消费者获得最大利益，保证消费者自由远离电话插座，甚至摆脱国家电话公司。

---

① “铱星”全球卫星电话系统最终因销售薄弱、经营成本过高以及技术上的小麻烦不断造成严重亏损，并于1999年8月宣告破产。——译者

拉丁美洲通过采用类似技术——以移动电话代替在农村架设电线和立电线杆——也在电话基础设施方面迅速赶了上来。1995年2月西方七国首脑会议在比利时布鲁塞尔召开期间，特莱迪斯克公司合伙人克莱格·麦克考承诺向发展中国家用户有偿开放他的网络。中国只有将近2万条电话线（原文如此——译者注），在这个令人难以置信的通讯市场上，潜在投资者们都被各种赚钱项目搞得晕头转向。中国通讯市场在未来十年之内规模要达到1000亿美元，俾使中国从史前电话阶段直接奔向高速数据传输阶段，新的光纤通讯将带来巨大的生意。越南距拉美和中国仅仅一步之遥。

最后的十字军

分析家们估计，到2000年，电讯市场将从1993年的6,000亿美元爆炸式地增长到一万亿美元。勿庸置疑，如此巨大的有计划的增长将使得国营和私营企业之间的竞争趋于白热化。这块全球市场蛋糕有三层，哪一层都难对付。

第一层是信息高速公路的干线部分。铺设这部分基础设施的预算最大；而且，不管用水泥、钢铁、或者光缆，都费用高昂。据欧洲委员会估计，要把高容量光缆铺进所有欧洲家庭，费用将达200万亿美元，两倍于在美国铺设光缆的估计费用。美国联邦政府打算分文不

出，让私营企业支付这张帐单。亚洲建设这项基础设施的计划支出也达1,000亿美元，人们不得不问：谁来建设这些网络？电话公司（其铜缆虽然不敷现代需要，但已经连接起四面八方）顽固地企图尽力保持它原有的不管什么垄断，而基于普遍解除管制的前景，有线公司和大型娱乐企业也都将在这个富饶的新市场安营扎寨，提供上网服务、电话服务以及某种形式的互动电视。人们渴望发送超出老式电缆能力的更多的信息，对以布线为形式的新基础设施的需要即渊源于此。要通过铜电话线发送一张达到播出质量的静止照片，可能需要七分钟。数以百万计的美国人都通过有线公司的同轴电缆收看有线电视，而只要电缆带宽更大，有线公司已铺设好的电缆发送同样一张达到播出质量的静止照片只要一秒钟时间。光缆前景亦撩人，其带宽甚至比同轴电缆更大，而且，就像许多企业希望的那样，可允许实时下载所有种类的媒体。不过，这些发展尚无定形。

美味的第二层信息市场蛋糕，是这些连接所要导入的硬件。这方面早已出现五花八门的设想和机器原型。设想中的机器以多媒体（能够操纵多种媒体）为主导，借助有庞大内存的硬盘、光盘驱动器或其它还没有想象出的手段，经数字整合，将电话、计算机和电视连成一体。1996年夏，苹果公司开始在日本销售“Pippin”电脑，这是第一款专门的因特网计算机，今后肯定会更多。

近来，有几家制造商引进了新型硬盘驱动器——压根儿不算是驱动器。PCMCIA（个人计算机记忆卡国际协会）卡不比信用卡更大，能够存储十亿字节信息，售价全在500美元上下。PCMCIA卡可插入许多计算机中的PCMCIA插槽，有着诱人的富有竞争性的产品名称，如“袖珍火箭”。目前，PCMCIA卡在摄影记者当中十分抢手，他们短缺内存的数码相机可以藉此把照片的有效载荷下载到方便轻盈的袖珍卡里。很难说PC卡技术会不会只是昙花一现，但更小、更强大的信息存储方法的迅速发展，兼以光纤技术提供的更大带宽，应当可以让因特网把所有各种需要大存储量的产品导入千家万户。许多对媒体反应快的人已经想到一项潜在用途，即选择离线观看电影，从因特网上把电影直接、实时下载到家里。支持者们设想这种未来机器兼有录像机的全部功能（暂停、前进、倒退）以及许多新功能，例如无论何种语言的电影，均能选择原始、配音译制或带字幕的版本。这些技术乐观主义者们预想出各种文化、教育产品和互动游戏。这个未来市场可能创造巨大的收入。

第三层蛋糕涉及信息提供商。在这个领域，如果欧洲正确出牌，措施得当，它能够大举进军数据库开发、在线销售等层出不穷的市场。

不过，首先消费者得把这个三层蛋糕给吞下去，而这可能引起严重的消化不良。这些潜在买主是建设网络社会的根基，但这个基础摇摇晃晃，并不牢靠。现在的

网虫们为网上服务付出的费用相对低廉。即便如此，谁知道将来的上网费用会是多少，又有多少消费者愿意付费呢？欧洲的电话费远比美国高。在曼哈顿从家里给朋友打市内电话，一个小时只要13美分，而在巴黎要3美元。毫无疑问，操纵消费者习惯、帮他们倒空钱包，再把钱装进投资者的保险箱里，在这方面企业家们是绝不会受到良心谴责的。

有一点十分确定：没人不冒风险。这是一座崭新的多媒体拉斯维加斯赌城，赌桌上的钱一直堆到天上去。信息业正在非常迅速地变成工业化国家的主打产业。举个疯狂的例子：比尔·盖茨和移动电话技术领袖克莱格·麦克考合伙创办了一家换了别的任何人都被认为是在发疯的企业——特莱迪斯克公司。该公司注册资本即超过90亿美元，两人计划在2001年前发射840颗微型卫星上天，以此作为全球数字声音和数据通讯网络的主干。不要多长时间，有电话的人只要随身携带一个号码就能打电话。不论是委内瑞拉的炼油厂，还是乞力马扎罗山巅，抑或是路易斯安那沿海的捕虾船，这个号码将伴随他走到天涯海角，而且通讯的技术质量十全十美，用户能够通过同一个电话听筒发送声音或计算机数据。特莱迪斯克公司和铱星公司之间势将出现激烈的竞争，但待硝烟散尽之后，消费者就能够摆脱室内电线以及电话公司的束缚。在欧洲各国及其他许多国家，电话公司都是由政府控制的。

这个新市场所能创造的财富数量是惊人的。有出色创意和拳头产品的“启动”公司正在资本化，就好像以前从来没有涉足过这个“下一个才最好”的市场空间。许多即将载入1995年史册的公司都是和因特网相关的软件公司。为利用这个新市场，它们力图使上网更容易、更快捷、麻烦更少、图形界面更清楚实用、搜索引擎更易掌握和使用，乃至最勉强的初学者也会立刻感到轻松自如。仅1995年一年，企业资本家就向这些公司投资两亿多美元，五倍于上一年的投资额。人们围绕着这个新兴信息社会正在构筑未来的全球经济。以网络社会为号召，信息战也正在酝酿和蓬勃发展，必定会对被抛到一旁的地区和人民造成严重灾难。华尔街对这个新时代里的任何机会，都准备着猛虎扑食一般扑过去，它用于技术问题的开支超出以往任何时候。1994年问世的优秀的因特网浏览器“网景”起初是由吉姆·克拉克在因特网上免费发布的，半年之内被下载了五百万份。克拉克后来让软件制作者马克·安德雷森及其签有合约的编程小组对软件进行改进，制作出更好的版本，但这回不免费了。以前用过这个软件的人没有几个打算放弃，软件卖得很火。对过去一直使用和网景性质相同的Netsite的服务提供商来说，他们的损失可就相当可观——在6000美元到20000美元之间。1995年8月9日，吉姆·克拉克的网景公司在纽约证券交易所公开上市，点燃因特网热潮的最后一根导火索。投资者们一窝蜂地

涌入交易所，买下了价值 21.3 亿美元的网景股票。网景问世仅仅十六个月之后，克拉克就成功地把他最初的 400 万美元投资变成一笔真正的财富。

长年在“班里最聪明的孩子”的赞誉声中长大的比尔·盖茨个人财富超过 100 亿美元（这使他成为除寥寥几个君主之外世界上最富有的人之一）。盖茨亲手封杀了网络空间里的所有竞争对手。他用来撬动市场的工具不是什么秘密，就是他和朋友保罗·艾伦创办的微软公司。微软公司总部设在西雅图，是世界上最强大的软件公司。盖茨于 1995 年 8 月推出视窗 95，从此他力图通过两样拳头产品控制市场：首先是专门的网络系统，称为微软网络系统；其次是为和网景竞争而设计的导航器“微软探险者”。1995 年 12 月，微软公司总裁盖茨重新定位了他的战略。基于生意兴隆，雇员达两万名，销售额达 60 亿美元，盖茨盯住一个首要目标：把因特网变成自家的新边疆，不让网景成为网上飘扬的唯一旗帜。盖茨把微软网络抛在脑后，为这个新重点全力以赴地奋战，终于在 1996 年 8 月公开了他的最新型战争武器：微软探险者 3 号，免费发布，一意与网景竞争。微软探险者 3 号在头一个星期就下载了一百万份。从那时起，微软便立于不败之地，一如既往地兴旺发达。微软探险者 4 号接着问世，而网景则如同加入了一场漫长、坎坷的赛跑。微软犹如一位马拉松健将，非常清楚如何以最快的速度冲向整个美国和世界其它地方。

结束语

战争正在进行，扛着计算机武器的大军在已经铺就的网络上挺进。迄今为止，他们属于精锐部队：美国先生和美国太太还没有在闹烘烘的房间、厨房和书斋里铺进光缆。美国人要把手伸进重型计算机武器库，还得再过几年。但他们会有那么一天的——阿·戈尔要求美国人全都进到信息高速公路上，全副武装，作好准备，向无限以远的信息进军。

这一革命具有许多不同寻常的特征，其中之一就是技术的相对普及。如果你想兜售信息，你可以在自家车库里（计算机）设一个捕鼠器（站点），用万维网开辟出到达它的路径，然后，就齐活儿了——你在夏威夷度假的照片、花园里鸟儿的啼鸣、数学方程式和音乐作曲、内衣裤一览表、乔叟中古英语作品全集、新闻快报和军事公报——万事乃至万万事，无不可以在网上进行，而且其中许多早就成为现实。

信息战业已爆发。计算机帮助人类通讯、理解、学

习，可能还促进了新型的全球民主。不过，旧世界秩序的拥戴者对此一点都不开心，什么事都极力要按他们年轻时候的游戏规则扭着来。但不论怎么说，运动场地是永远改变了，他们那套游戏规则再也不适用。皮埃尔·列维提醒我们："总的说来，权力和世界真正的运作方式没有多少亲合力……权力总是力图永远保持优势，把住既得利益，维持现状，左堵右塞——在迅速的大规模衰败时期，这些都是危险目标。"

无疑，野蛮的冲突仍然在撕裂文化、土地和人民。不管是石器时代还是信息时代，看来它们都无消失之望。但在世界其它地方，战争在改变形式，而且找到了新战场。世界民主国家的军队正在成为笨拙的管家婆，为维持摇摇欲坠的现状而苦苦挣扎。

信息是这场游戏的名称。信息在被购买、出售、监视、玩弄和学习；信息（真真假假）正在大量地四处流传；信息在制造财富，也使财富遭到偷盗。我们实际上还不清楚，一旦所有一切都被说出做到，一旦所有道路都被铺就，到那时，信息高速公路将把我们带向何方？不过，在各行各业，新规则早就在发挥作用。因特网先驱们想让因特网成为全世界人民的活动天地，成为富有而自由的乌托邦。这些快乐的空想家们不希望自己的因特网婴儿堕落成资本主义喂养狂。他们希望因特网保持最初的本来面目，依然是人们通讯和免费交换信息的场所，不必惧怕私人侦探。他们希望人们都懂得，因特网

是志同道合的人们聚集的地方，而不仅是蹩脚的内容供应商、开发商之流的另一个牟利的口实。

但当然啦，谍报机构可根本不这么看问题，他们想利用因特网楔入我们的私生活。他们叫嚷说，他们现在有能力防大患于未然了，以此来证明他们侵犯公民隐私有正当道理。他们相信，凭借国家安全的名义，他们就应该有权利随时随地东张西望，尽管这种行径可能侵犯了个人自由。新网络业已成为难以置信的调查手段。如果不论网民如何激烈反对，谍报机构仍然设法得到了阅读所有电子通讯的权利和手段，就像阅读打开的书一样；并且设法禁止人们使用它所不能破解的加密方法，那么民主的基础肯定就开始大大动摇了。

军队作为加密通讯的先行者，已经全面地接受了网络逻辑。网络工具赋予人类如此丰富的促进民主和人际交流的能力，但军队却把它看成是争夺信息霸权的新的理想的战争武器。他们这方面至少是正确的。黑客能够造成某些严重破坏。虽然强中自有更强手，正在严阵以待他们的到来，但因特网还是从这些袭击中得到了教训。人们依然拭目以待的是军队将如何利用因特网发起攻击；而且，在什么样的情况下，这类战役会打响。

在美国，那些维护电子地球上的完整人权的人，正在和打着所谓的进步旗号、谋求某些特权的新网络秩序鼓吹者之间发生正面冲突。而且，由于网络发展的速度，这些冲突不久就将蔓延到因特网触角所至的每个地方。正在发生影响

的一个重大矛盾是，因特网迅速变得似是而非起来：它既是一曲民主交流的即时赞歌，又是系统地压制个人自由的样板。在日本，网络观念公然违反了政府进行社会控制的传统，而这种政府还在台上，并且阻遏了网络的壮大发展。日本可能以这种方式受到更好的保护，免于遭受全球多向通讯的潜在的负面影响。有些公司很大程度上也是以这种方式，通过禁止雇员登录上网以避免受到不良影响——节制总归是最安全的选择。但是，真的有人能抵御这股潮流吗？学者尼古拉斯·内格罗蓬特不这么认为。他说："变革的动力将来自因特网。这句话，既可以照字面意义理解，也可以当成是在举例或者打比方。因特网引人入胜，它不仅是广泛的深入的全球网络，也是某种演变的样板。而且这种演变显然没有主管设计师，它的形态很像是一群野鸭，谁都不是老板，所有"鸭子"到目前为止都可惊可佩。"

把因特网视为变革动力，这是否评价过高了？对此时间自会作出判断。对已经和即将上网的人们来说，现在最重要的是要知道存在什么危险。当前，因特网形式还很初级，但即便如此，它显然正在对我们的日常生活和社会产生强大的冲击，就像我们已经看到和听到的那样。网民们已经习惯于生活在这样一个世界里——在那里，距离有等于无，只消轻触一键，砖墙就能变成一捅就破的纸。将来，这些变化只会日趋显著：个人自由和民主将受到考验，并且将前所未有地更加强大。但现在，战争距离胜利之日仍然"路漫漫其修远兮。"

参考书目

1. Katie Haffner & Matthew Lyon, Where Wizards Stay up Late: The Origins of the Internet, Simon and Schuster, New York, 1996

2. Claude Silberzahn with Jean Guisnel, Au coeur de secret, 1500 jours aux commandes de la DGSE 1989/1993, Fayard, Paris, 1995

3. James Bamford, The Puzzle Palace, Houghton Mifflin Company, New York, 1982

4. David Kahn, Seizing the Enigma: The Race to Break the German U - Boot Codes, 1939 - 1943, Houghton Mifflin Company, New York, 1991

5. F. H. Hinsley and Alan Stripp, Code Breakers, the Inside Story of Bletchey Park, Oxford University Press, London, 1993

6. Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Johns Willey and Sons, New

York, 1994

7. William Stallings, Protect Your Privacy: The PGP User's Guide, forwarded by Philip Zimmerman, National Computer Security Association, 1995

8. Bruce Sterling, The Hacker Crackdown: Law and Disorder on the Electronic Frontier, Bantam Books, New York, 1992

9. Steven Levy, Hackers, Heroes of the Computer Revolution, Belta Books, New York, 1994

10. Michelle Slatalla and Joshua Quittner, Masters of Deception: The Gang That Ruled Cyberspace, Harper Perennial, New York, 1995

11. Winn Schwartau, Information Warfare: Chaos on the Electronic Superhighway, Thunder's Mouth Press, New York, 1994

12. Katie Haffner and John Markoff, Cyberpunk, Outlaws and Hackers on the Computer Frontier, New York, 1991; Last Edition, with a postface by Katie Haffner, Touchstone, New York, 1995

13. Tsutomu Shimomura and John Markoff, Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw, by the Man Who Did It, Hyperion, New York, 1996

14. Jonathan Littman, The Fugitive Game, Online with

Kevin Mitnick, Little, Brown and Company, New York, 1996

15. Clifford Stoll's Bestseller, The Cuckoo's Egg, Doubleday, New York, 1989

16. David Wise, The Nightmover: How Aldrich Ames Sold the CIA to the KGB for $4.6 Million, HarperCollins, New York, 1995

17. Peter Earley, Confessions of a Spy: The Real Story of Aldrich Ames, G. P. Putnam and Sons, New York, 1997

18. Deborah Russel and G. T. Gangemi Sr., Computer Security Basics, O'Reilly and Associates, Sebastopol, CA, 1992

19. Winn Schwartau, Terminal Compromise, You can read the book on Winn's website: www.infowar.com

20. Claude – Marie Vadrot and Louisette Gouverne, Tous fiches, First, Paris, 1994

21. Mark Knobel, "Internet: nouvelle communication utilisee par les extremists racists et xenophobes?" in CNCKH, "Le reseau internet et les droits de l' homme," Paris, 1996

22. Dominique Wolton, War Game, Flammarion, Paris, 1991

23. Alan D. Campen, The First Information War, the Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War, AFCEA International Press, Fairfax, VA, 1992

24. Alvin Toffler, The Third Wave, William Morrow and Company, New York, 1980

25. Zaki Laidi, Un monde prive de sens, Fayard, Paris, 1994

26. Martin Shaw, Post - Military Society, Polity Press, Cambridge, 1991

27. John Mueller, Retreat from Doomsday. The Obsolescence of Major Wars, Basic Books, New York, 1989

28. Jean - Louis DuFour and Maurice Vaise, La Guerre au XX siècle, Hachette, Paris, 1993

29. Alvin and Heidi Toffler, War and Anti - war: Survival at the Dawn of the 21st Century, Little, Brown and Company, New York, 1993

30. Bruno Martinet and Yves - Michel Marti, L'intelligence dconomique. Les yeux et les oreilles de l'entreprise, Editions d'organisation, Paris, 1995

31. Pierre Levy and Michel Authier, with preface by Michel Serres, Les arbies de connaissance La Decouverte, Paris, 1992

32. Christian Harbulot, La machine de guerre economique: Etats - Unis, Japon, Europe, Economica, Paris, 1992

33. Robert Dreyfuss, The CIA has opened a global Pandora's box by spying on foreign competitors of American

companies, Mother Jones, 1994

34. Francois Jakobiak, Pratique de la veille technologique, Editions d'organisaton, Paris, 1991

35. Nicholas Negroponte, Being Digital, Alfred A. Knpf, New York, 1995

36. Pierre Levy, Collective Intelligence, Plenum Trade, New York, 1997

[General Information]
书名=互联网上的间谍战
作者=(法)让·吉内尔(JeanGuisnel)著
页数=243
SS号=0
出版日期=